CLAIMS SECTION: All active claims with (STATUS), lastly any newly submitted claims: 66 - 103 (NEW).

We claim:

1. - 28. (CANCELLED).

29 - 65 (CANCELLED).

66. (NEW) A specific process for doing public key cryptography over an open systems networking architecture in a relatively low probability of hacker breaches or a cryptographically secure manner, meant for safeguarding relative commercially valued, multi-million dollar digital masters, which open systems network architecture includes existing lower abstraction cryptography system layer, prior art and new art components, integrated into a specific new invention system process patent of a higher abstraction cryptography system layer, new public key cryptography systems level, architecture, comprising of the steps of:

providing of the component of: prior art, a tamper-resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], with means for tamper resistant, solid state, permanent memory storage,

providing of the component of: a static random access memory [SRAM], with means for non-permanent solid state memory storage,

providing of the component of: prior art, a dynamic random access memory [DRAM], with means for volatile solid state memory storage,

providing of the component of: prior art, cryptographic micro-controller [C-u-Ctlr], with means for secure storage of cryptographic keys contained in provided, said prior art, tamper resistant non-volatile permanent memory [TNV-EEPROM], plus other cryptographic hardware aids for strong cryptography,

providing of the component of: prior art, the smart card used for media ticket applications containing provided, said prior art, cryptographic micro-controllers [C-u-Ctlr's], furthermore, which already have contained provided, said prior art, tamper resistant, non-volatile, electrically erasable programmable read only memory [TNV-EEPROM],

providing of the component of: new art, a smart card with bio-ID, used for media ticket applications containing provided, said, prior art, cryptographic micro-controllers [C-u-Ctlr's], furthermore, already containing provided said, prior art, tamper resistant, non-volatile electrically erasable programmable read only memory [TNV-EEPROM] as used for cryptographic key storage,

providing of the component of: prior art, serial data computer communications interfaces,

providing of the component of: prior art, a smart card reader, with means for reading said smart card,

providing of the component of: prior art, biological-identification readier [BIO-ID-READER] means which attach to personal computers [PC's], with bio-ID means such as: digitized fingerprint readers, digitized iris scan readers, digitized facial cognitive features readers, digitized DNA readers,

providing of the component of: prior art, an internet protocol [IP], wide area network [IP WAN],

providing of the component of: prior art, a world wide web server [WWW] or web or graphics rich portion of the Internet web server computer,

providing of the component of: prior art, a personal computer [PC], which is non-cryptographically secure,

providing of the component of: prior art, a personal computer [PC] web client,

providing of the component of: prior art, a personal computer [PC] peripherals,

providing of the component of: prior art, a data entry devices of an on-board protected electronic device, toggle field with a prior art liquid crystal display [LCD] for entry of the unique customer passphrase with closely corresponding passcode entry;

providing of the component of: prior art, a data entry device of computer keyboards,

providing of the component of: new art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-text data sent to an attached provided, said prior art, digital serial bus, furthermore, 1st example means being digitized fingerprint bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of: prior art, a banked-EEPROM card reader-writer,

providing of the component of: prior art, a personal computer's [PC's] peripheral data storage devices, with means for detachable or removable provided, said prior art, tamper resistant, non-volatile, electrically erasable programmable read only memory [TNV-EEPROM] removable memory module units,

providing of the component of: prior art, a personal computer's [PC's] based peripheral data storage media units, with means for archival storage of large amounts of digital data,

providing of the component of: prior art, a cryptographic digital signal processor [C-DSP],

providing of the component of: a new art, a cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through provided, said prior art, tamper resistant non-volatile memory [TNV-EEPROM],

providing of the component of: new art, cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through provided, said prior art, tamper resistant non-volatile memory [TNV-EEPROM], furthermore, through enhanced cryptographic hardware aids and secure or anti-hacker, firmware aids, for both secret key and for public key, strong cryptography,

providing of the component of: a new art, programmable gate array logic [GAL] form of high density, application specific integrated circuit [ASIC] with embedded, provided said, new art, cryptographic digital signal processor [C-DSP] structural means, furthermore, with functional means as mentioned in the paragraph just above,

providing of the component of: a new art, cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through provided said, prior art, tamper resistant non-volatile memory [TNV-EEPROM], furthermore, through enhanced strong cryptographic algorithm, hardware aids, for both secret key and for public key, strong cryptography, furthermore, with

hardware and firmware support for modern secret key ciphers such as the Advanced Encryption Standard [AES] cipher stressing variable length secret key strength,

providing of the component of: prior art, a non-cryptographic micro-processor [uP] or a central processing unit [CPU], with exampled implementation means such as a commercial, 32-bit, Intel Pentium class of micro-processor central processing unit [CPU], with a control unit and on-chip floating point processing unit,

providing of the component of: a new art, a cryptographic computing based unit [C-uP], furthermore, having a hardware design implementation of a proper subset or silicon compiler class library selection, of said cryptographic micro-controller [C-u-CTLR], with means for secure handling of strong cryptography keys and auxiliary strong cryptography hardware aids, furthermore, with proper subset functionality of the provided, said cryptographic digital signal processor [C-DSP] structural means,

providing of the component of: a new art, a cryptographic computing based unit [C-uP], furthermore, with structural means for secure handling of strong cryptography keys by provided said, prior art, tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], intended for commercial digitally compressed, digital music and movies, furthermore, having a hardware design implementation of a proper subset or silicon compiler class library selection, of provided, said new art, cryptographic digital signal processing [C-DSP] structural means,

providing of a new art, class of cryptographic computing hardware integrated circuit [C-IC] units or a provided, said cryptographic digital signal processor [C-DSP] structural means, comprising of the above exampled cryptographic digital signal processor [C-DSP] structural means, plus very similar in hardware design given modern grey scales of very cost competitive, digital chip architectures, ranging in relevance, from design bench, custom fuse link programmable, application specific integrated circuits [ASIC'S], all the way in grey scale digital computing complexity, to modern silicon compiler custom designed integrated circuits [IC's] for mass production, as structural implementation hardware means, only illustrated by the above cryptographic hardware units, with functional means for keeping strong cryptography: secret keys, private keys, family keys, session keys, and often used public keys, secret in provided, said prior art, tamper resistant, non-volatile electrically erasable programmable read only memory [TNV-EEPROM], furthermore, in a class of so called, tamper resistant hardware, or red-black hardware, furthermore, with structural means of using pass-thru encryption methods over open or wiretapable digital computer system buses, in order to confidentially and securely, transfer said strong cryptography keys into the said tamper resistant hardware, from an external wiretapable, input-output [I/O] digital serial data bus, connecting of data source only exampled by a human portable vault functional means, structural means of a smart card, and its own provided, said prior art, tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], furthermore, also exampled by a remote local area network [LAN] source,

furthermore, also exampled by a MODEM connected remote global Internet-Web source,

providing of the component of: a new art, a non-cryptographic, media player [MP] having internal, provided said prior art, digital signal processors [DSP's],

providing of the component of: a new art, a cryptographic media player [C-MP], constructed with a provided said, new art, cryptographic digital signal processor [C-DSP] structural means, having structural means for internal provided said, tamper resistant non-volatile, electrically erasable programmable read only memory [TNV-EEPROM], for playing of customized per customer, strong encrypted digital media,

providing of the component of: a new art, cryptographic media player [C-MP], with means for playing back custom secret key encrypted, compressed digital, audio-video in standard format,

providing of the component of: a new art, cryptographic personal computer [C-PC] which is created by using provided, said new art, said cryptographic micro-processor [C-uP], with means for digitally processing, new art, custom encrypted digital media,

providing of the component of: a new art, cryptographic personal computer [C-PC] having a subset functionality of provided, said new art, cryptographic micro-processor [C-uP] structural means, which is created by using a prior art, standard off-the shelf, personal computer [PC] design with a new art, said cryptographic micro-processor unit [C-uP],

providing of the component of a new art, cryptographic operating system [C-OS], designed for provided said, new art, cryptographic personal computer [C-PC] having an internal provided said, new art, cryptographic micro-processor unit [C-uP],

providing of the component of: new art, a universal cryptographic set-top box, form of provided said, cryptographic media players [C-MP's] structural means, used for playing back customized digital media,

providing of the component of: a new art, cryptographic micro-mirror module [C-MMM], commercial theater projection-theater sound units which are special provided, said new art, cryptographic media players structural means, furthermore, which use prior art, removable permanent memory devices,

providing of the component of: new art, a modified secure or cryptographic or red-black operating system [C-OS] for world wide web

[WWW] server computers, which will custom 1-time use only, customer session key encrypt, a vendor secret key encrypted digital media master, and electronically distribute custom, encrypted digital media masters, furthermore, using prior art, of firewalls, anti-viral software updated weekly, using network protocol converters, using standard layered security methods, and using prior art, 'inner sanctum' data processing security procedures, protection for vendor session key or 1-time use only, secret key encrypted digital media masters,

providing of the component of: prior art, a global Internet and world wide web [WWW] based transmission control protocol-internet protocol [TCP-IP] command protocol stack program for Internet connectivity,

providing of the component of: prior art, standard, a plurality of cryptographic mathematics algorithms,

providing of the component of: prior art, a plurality of public key cryptography algorithms which create public keys and private keys,

providing of the component of: prior art, a plurality of secret key cryptography algorithms which create secret keys and session keys or 1-time use only, secret keys, and also play counts or access counts or media decryption counts and play codes or session keys or 1-time use only secret keys,

providing of the component of: prior art, a plurality of hybrid key cryptography algorithms which are combined public key and private key cryptography algorithms,

providing of the component of: prior art, a plurality of private key and secret key splitting algorithms,

providing of the component of: prior art, a plurality of private key and secret key escrow techniques,

providing of the component of: prior art, a plurality of algorithms used to generate: cryptographic keys which are the collective public keys, private keys, secret keys, session keys or 1-time use only secret keys, play counts, play codes, passphrases-passcodes,

providing of the component of: prior art, a plurality of computer cryptography protocols,

providing of the component of: prior art, a plurality of pass-thru encryption algorithms for transmitting secure data over wiretapable computer buses ['red buses'],

providing of the component of: prior art, standardized form, a plurality of lossy compressed digital media algorithms with many prior art example means, and new art emerging future standards,

providing of the component of: prior art, a transmissions control protocol/internet protocol [TCP/IP] for Internet connectivity,

providing of the component of: prior art, a secure internet protocol layer [secure IP layer] layer of Internet data encryption, used in this present patent only as an outer-most security layer which is considered cryptographically un-reliable,

providing of the component of: prior art, a secure sockets layer [SSL] layer of Internet data encryption,

providing of the component of: prior art, a plurality of world wide web [WWW] server standard interchange file language with first example protocol being hyper-text mark-up language [HTML], second example protocol being extensible business mark-up language [XBML] also known as [XML], and third example protocol being the most generalized-text mark-up language [GTML],

providing of the component of: a plurality of world wide web [WWW] client standard interchange file languages, with first example being hyper-text mark-up language [HTML],

generating of a set of common system keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using provided prior art said public key and secret key cryptography algorithms to generate system cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding of generated said common system keys into each and every provided, said cryptographic digital signal processor [C-DSP]

structural means, and also if relevant, a provided said cryptographic integrated circuit [C-IC], furthermore, embedding said common system keys into the said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM] inside of each and every, provided said smart card,

generating of a set of unique per vendor, commonly distributed only in provided, said tamper resistant hardware [TNV-EEPROM], media distribution vendor cryptographic keys eventually used in a provided said, new art, cryptographic digital signal processor [C-DSP] structural means, and also if relevant, a provided said, new art,, cryptographic integrated circuit [C-IC], involving several processes with a 1st example prior art, provided, said, being the US National Institute for Standards and Technology's Clipper-Capstone chip with provided, said embedded tamper resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], and a 2nd example provided said, new art, cryptographic digital signal processor (C-DSP) structural means being a prior art, digital signal processor having a silicon compiler designed equivalent of the former's functions [C-DSP] structural means, with added silicon compiler functions for prior art algorithm means for subsequent customer uses of digital signal compression audio-video digital compression means involving several processes and components with 1st example audio-video digital compression means involving several processes being given as prior art, Moving Picture Electronics Group standards X [MPEG X], 2nd example audio-video digital compression means being given as prior art, fast wavelet audio-video compression or

convolutional coding compression, 3rd example audio only digital compression example means being given as prior art, MPEG I audio layer 3 [MP3], and 4th example audio only digital compression example means being given as prior art, fast wavelet audio only compression algorithms [AAC], furthermore, with subsequent customer uses of a prior art, pass-thru encryption means involving several processes and components which are used to transfer said unique customer cryptographic keys over wirctapablc or opcn computcr buscs ['rcd buses'] with a first example pass-thru encryption means given as common, family key, secret key encryption, a second example pass-thru encryption means given as common family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor public keys followed by the relevant vendor public key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor public keys followed by relevant vendor private key decryption of the received data block, and a third example pass-thru encryption means being a family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor secret keys followed by the relevant vendor secret key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor secret keys followed by relevant vendor secret key decryption, for eventual manufacturing into a cryptographic media player, which is the process done by the media ticket smart card system authority's, party s's, dedicated

public key generation authority, party g, using prior art algorithms for both public key and secret key cryptography to generate a unique set of vendor cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding in entirety, said unique set of vendor cryptographic keys in an organizational table form means involving several processes with first example organizational table form means being a unique vendor system key table which is indexed by a vendor identification number, furthermore, said organizational table form means is semi-conductor foundry factory embedded into each and every cryptographic digital signal processor [C-DSP] structural means, while specific vendor private keys and vendor secret keys including a minimum count of one vendor key of the private key of vendor party vn, are factory time embedded into each and every one of vendor party vn's eventually distributed provided, said media ticket smart cards and their internal, provided, said cryptographic micro-controller [C-u-Ctlr] for use in a pass-thru encryption means of several example pass-thru encryption means as explained in a separate process,

generating of a unique media ticket smart card cryptographic key set or also known as a given, unique customer party a's, chosen out of the unique customer parties: a, b, c, i to z's, cryptography key set, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using provided, prior art algorithms for both public key and secret key cryptography to generate unique customer cryptographic keys, while having absolutely no access to customer identifications,

furthermore, the sub-process of embedding into a provided, single said unique media ticket smart card with an embedded cryptographic micro-processor (c-uP), a unique customer party a's, unique cryptographic key into party a's, eventually distributed provided, said media ticket smart card with its internal cryptographically secure storage of provided, said embedded cryptographic micro-processor [C-uP],

distributing of the provided, said cryptographic digital signal processor [C-DSP] structural means, furthermore, the distributing of the provided, said cryptographic digital signal processor [C-DSP] structural means, is based upon the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing provided, said cryptographic digital signal processor [C-DSP] structural means, to individual media distribution vendors for manufacturing into vendor party vn's cryptographic media players while having absolutely no access to whole cryptographic keys and having unique vendor party vn access to only his own unique vendor secret key vn, and unique vendor private key vn, with its unique, matching public key vn,

distributing of the factory cryptographically pre-programmed, provided, said media ticket smart cards, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing the provided, said media ticket smart cards, to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys,

escrowing of the split cryptographic keys which is the process done by the centralized, highly federated, public key generation authority, party g, safe-guarding the split cryptographic customer keys, and split cryptographic vendor keys in an entirely secure and confidential manner for achievement of legal means involving several processes, with a first example legal means being simple customer identification and lost cryptographic key recovery, a second example legal means being court ordered only, disputed ownership cryptographic key recovery, and a third example legal means being court ordered only cryptographic key recovery use by law enforcement,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with a minimum of 3-layers of digital computer architecture: a bottom-most layer of the relevant patent drawing, composed of the media ticket smart card system authority, a middle layer composed of authorized media distribution companies labeled as parties vn, and a top-most layer or user layer composed of customer parties: a, b, c, i to z,

preparing of a unique play code and a unique play count which is the process done by the authorized digital media distribution unique vendor company, party vn, preparing said unique play code [a session key or one-time use secret key], and said unique play counts [a paid for number of plays or count of free trial plays], and preparing of the custom encrypted digital media for downloading to each customer,

downloading to unique customer parties, a, b, c, or i to z, at a private dwelling, prior art, insecure ['red bus'], personal computer [PC] which is the process done by the authorized digital media distribution vendor, party vn, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a centralized, highly federated, media distribution authority party s, hosted on a prior art, provided, world wide web [WWW] server over the global Internet to multiple prior art, provided, personal computer [PC] based web clients, one of whom is customer party, a, b, c, or i to z, of encrypted play codes (one-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into said factory cryptographically programmed, prior art, provided, media ticket smart cards attached to prior art, provided, personal computer (PC based) media ticket smart card readers, and one-way transfer of custom session key or one-time use only secret-key encrypted pre-unique vendor secret key encrypted digital media for deposit into physical digital media inserted into media drives attached to prior art, provided, customer personal computers (PC's),

delivering by foot which is the process done by the unique customer party a, of physically transferring both physical custom encrypted digital media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, prior art, provided, personal computer [PC] to any person's said cryptographic media player with its embedded said cryptographic digital signal processor (C-DSP) means, also with a built-in media ticket smart card reader,

encrypting in a pass-thru manner for media ticket smart card upload to a prior art, provided, cryptographic media player means with its embedded provided, said cryptographic digital signal processor [C-DSP] structural means, using pass-thru encrypting means involving several processes and components for transferring any type of digital data securely from originating said media ticket smart card up to answering provided, said cryptographic digital signal processor [C-DSP] structural means, with a first example pass-thru encrypting means being said common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, a second example pass-thru encrypting means being originate vendor, unique, vendor private key digital signaturing to 'signatured-text (not encrypted text thus readable by any party)' followed by answering vendor, unique, vendor public key digital public key encryption to 'cipher-text (encrypted text)' using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being a row, column table indexed by a vendor identification number, a third example pass-thru encrypting means being originate vendor, unique, vendor secret key encryption to 'cipher-text (encrypted text which combines signaturing)' using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being a row, column table indexed by a vendor identification number,

encrypting in a pass-thru return manner for said cryptographic media player's prior art, provided, embedded said cryptographic digital signal processor [C-DSP] structural means download to said media ticket smart card using pass-thru encrypting return means involving several processes and components for transferring any type of digital data securely from said cryptographic digital signal processor [C-DSP] structural means to said media ticket smart card with a first example pass-thru encrypting return means being common family key or shared secret key encryption which is known vulnerable to a single point of failure, second example pass-thru encrypting return means being answer vendor unique private key digital signaturing to 'signatured-text' or digitally signatured text which is non-encrypted, and thus readable by any party, followed by originate vendor unique public key encryption to 'cipher-text' or encrypted text using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being the row, column table indexed by a vendor identification number, a third example pass-thru encrypting return means being answer vendor unique secret key encryption to 'cipher-text' or encrypted text, which combines digital signaturing by using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being the row, column table indexed by a vendor identification number,

initializing before playing which is the process done by the given customer, party a, of preparing any customer party's: a, b, c, i to z, personally owned provided, said new art, cryptographic media player, with its internal, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, by inserting his given own party a's, unique custom encrypted digital media, and also by inserting his given, own party a's unique provided, said media ticket smart card,

authenticating by customer triangle authentication which is the process done by provided said, new art, cryptographic media player [C-MP] structural means, with its provided, said embedded said cryptographic digital signal processor [C-DSP] structural means, which process step may be skipped for low security only when customer time and effort is of the essence,

transferring of the cryptographic keys from the prior art, provided, said media ticket smart card to provided said, new art, cryptographic media player having its prior art, provided, embedded said cryptographic digital signal processor (C-DSP) structural means, by use of said pass-thru encrypting means, of the unique customer cryptographic keys over wiretapable or open computer buses ('red buses') which is the process done by the cryptographic media player to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n which are pass-thru encrypted by the several pass-thru encryption means involving several processes and components for transfer over wiretapable computer buses ('red buses') to the player's own cryptographic memory (TNV-EEPROM)

for access by its cryptographic digital signal processor (C-DSP) means, with said first example pass-thru encryption means being the common family key encryption vulnerable to a single point of attack, a said second example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said third means of pass-thru encryption being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access,

transferring of the cryptographic keys away from provided said, new art, cryptographic media player having its embedded said cryptographic digital signal processor (C-DSP) means to said media ticket smart card by pass-thru encrypting return means of the unique customer cryptographic keys over wiretapable or open computer buses ('red buses') which is the process done by the cryptographic media player which are pass-thru encrypted by the several pass-thru encryption means for transmit using it's cryptographic digital signal processor (C-DSP) means, the encrypted play codes with header and encrypted play counts with header both with cryptographic digital signal processor (C-DSP) means incremented sequence counts (to avoid recorded replay attacks without the use of synchronized digital clocks) to the media ticket smart card A transferred over wiretapable computer buses, with said first example pass-thru encryption means being the common family key encryption vulnerable to a single point

of attack, a said second example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said third means of pass-thru encryption being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access,

authenticating using media triangle authentication which is the process of matching the unique digital media with its matching unique play code by the method done by said cryptographic media player's embedded said cryptographic digital signal processor doing digital media triangle authentication using sample reads of test data with successful decryption,

cryptographing using hybrid key cryptography which is the process done by provided said, new art, cryptographic media player's [C-MP's], embedded provided, said cryptographic digital signal processor [C-DSP] structural means, using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys [ssk-n], used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own provided, said tamper resistant, non-volatile memory [TNV-EEPROM] embedded on his provided, said cryptographic digital signal processing [C-DSP]

structural means, with a 1st example means of the provided said, new art, cryptographic digital signal processor [C-DSP] structural means, and a 2nd example means of a provided, said cryptographic integrated circuit [C-IC], which said 1-time use only secret keys or session keys, may be later stored in provided, said tamper resistant non-volatile memory [TNV-EEPROM], embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts,

accounting by provided said cryptographic media player's embedded, provided, said cryptographic digital signal processor [C-DSP] structural means, which is the process done using hybrid key cryptography digital media playing of one-way transfer of custom session key encrypted digital media, owned by unique customer party a, in a controlled access manner mostly for financial accounting purposes which uses the play codes [session key or one-time secret key] and play counts [paid for number of plays or count of free trial plays] contained in media ticket smart cards,

playing by provided, said cryptographic media player having its embedded, provided, said cryptographic digital signal processor [C-DSP] structural means which is the process done using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or one-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor (C-DSP) means and also the hardware secret key double decryption directly used upon the custom encrypted, one-way transfer

of custom session key encrypted digital media which is pre-unique vendor secret key encrypted, using first the unique customer session key decryption and then the unique vendor secret key decryption with sequence number checks for countering recorded replay attacks,

escrowing retrieval of lost, stolen, or disputed legal ownership provided, said media ticket smart cards. as well as custom, cipher text, digital media distribution material, which is the process done by the given, unique customer, party a, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of 'de facto,' and then internationally standardized cryptography sanctioned by industry trade groups such as the Recording Industry Association of America's [RIAA's] Secure Digital Music Initiative [SDMI], and the National Association of Broadcaster's [NAB's] Secure Digital Broadcast Group [SDBG],

whereby the present invention has implemented through the minimal said 3-layer federated system of cryptographic layers of the relevant patent drawing, while counting for the purposes of this patent process claim a widened scope, combined 2 drawing layers to 1 process claim layer, combining the low-middle and high-middle said drawing layers of the relevant patent drawing into a single middle said this claims layer, thus combining for claims purposes, the commercial hardware vendor parties, parties vn, and a low-middle layer for commercial digital media vendors, parties vn, furthermore, the full process is re-

inforced or 100% supported, of a design rule, of having no inherent hardware and firmware secrecy, no hidden wiretapping points, and also no double key spaces, furthermore, the minimal said 3-layer federated system of cryptographic this claims layers, of this invention's layers: the highest cryptographic system architecture layer of said system keys under said system party s, comprising of: whole key generation party g, optional by dependent claims to this independent claim, only for customer convenience and legal purposes, split key escrow minimal of 2 parties en, and commercial customer identification known distribution party d, in which this system party s's administration through said whole key generation party g, has been given 100% whole key knowledge, but, 0% knowledge of customer identifications, furthermore, minimal of 2 split key escrow parties en, also has optional, said split keys, who have knowledge of only 1/N, integer N greater than 2 being the total count of the system party s authorized, split key escrow parties en, or 1/N split cryptographic key knowledge, while never having been given by party s any whole cryptographic key knowledge, nor parties en having been given any customer identification [C-ID] knowledge, furthermore, said party s also having been given by said whole key distribution party d, who has been given 0% whole key knowledge, but, having been given 100% knowledge of customer identifications [ID's], furthermore, the use of provided, said tamper resistant non-volatile programmable read only memory [TNV-EEPROM] inside of provided, said media ticket smart cards, and provided said cryptographic digital signal processors [C-DSP's] structural means, also provided said cryptographic integrated circuit [C-IC] structural means, has been used to securely through crypto hardware, securely group distribute, whole cryptographic keys of

both: the vendor parties vn, whole vendor parties vn cryptographic keys in provided said, cryptographic digital signal processor [C-DSP] structural means, and also the customer party's a, b, c, i to z, individual and unique, whole cryptographic secret keys in provided said media ticket smart cards,

whereby the present invention has created several secure strong cryptography combined with provided said hardware architecture components, integrated into strong cryptography processes for doing unique, customer custom session key or one-time secret key encrypted copies of initially unique, vendor secret key encrypted, digital media distribution over the prior art, insecure ['red bus'] Internet using secure, World Wide Web (WWW) ['black'] servers involving the cryptographically secure transfer ['download'] from Web server to customer prior art, personal computers [PC's] over insecure ['red bus'] internet connection lines, of custom encrypted, digital media to prior art, standard form recordable media, and also custom decryption cryptographic keys ['play codes'] and custom pre-programmed accounting counts ['play counts'] for deposit onto prior art, smart cards called media ticket smart cards,

whereby the present invention has created several processes for securely physically transferring ['footprint download'] of both said custom, encrypted digital media on standard form recordable media along with the customer's universal media ticket smart card for all vendors and all digital media, to provided, said cryptographic media players [C-MP] structural means,, having embedded pre-programmed prior art, provided, said cryptographic digital signal processors [C-DSP's] for

media playing which are universally and uniquely, pre-programmed for every authorized vendor participating in the system, and can also accept any authorized, unique customer's smart card which must have relevant play codes and play counts for upload and use which are both uniquely matched to the authorized custom encrypted digital media inserted for playing,

whereby the present invention has achieved a highly federated or regional cryptography architecture is commercially implemented by this process used for commercial industry organizations, at said middle cryptography layer, in human corporate organization, proximately corresponding to today's US based, prior art, magnetic strip credit card management and distribution industry group associations, with corresponding EU based prior art, smart card commercial corporate organizations, furthermore, implementing through the process of this patent, over the global internet-web, individual human level and corporate body human level, trust granting policies known as a relative, two-way, middle level individual-organizational trust granting model [highly federated, 2-way middle level trust model], versus, earlier prior art, highly centralized, 100% top-down trust granting models exampled by the US Federal National Institute of Standard's (NIST's) Clipper chip and Capstone program, versus, earlier prior art, 100% bottom-up and 100% add-on PC software, trust granting models, often called tangled web of trust models,

whereby the present invention has implemented several of the above comprised systems processes, used in safeguarding relative, commercial

value, of multi-million dollar digital masters, released by vendors through World Wide Web (WWW) distribution.

67. (MEW). The invention and processes of claim 66 whereby the process or methods steps of generating of a set of common system keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using prior art algorithms for both public key and secret key cryptography to generate system cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding said common system keys into each and every provided said cryptographic digital signal processor [C-DSP] structural means, and also provided said cryptographic integrated circuit device class [C-IC's], furthermore, embedding said common system keys into each and every smart card, which is accomplished by the sub-steps of:

generating of prior art, a system secret, system family key [fak-F], with 1st functional use as an exampled means of pass-thru encryption, with 2nd functional use as an exampled means of secure centralized, cryptographic key generation,

generating of prior art, a system initialization vector [IV], furthermore, with 1st functional means for use as an initialization vector [IV] seeded, system message authentication cipher [MAC], furthermore, with 2nd functional means for doing confidential or classified message authentication cipher [MAC] verifications,

whereby this process claim has achieved a highly federated cryptographic system architecture's only top-most layer is implemented by this process using: secret secure whole cryptographic system key being secretly centrally generated by trusted system party s's, sole key generation party g, having knowledge of whole cryptographic keys but absolutely no knowledge of customer identifications [ID's], while also by party g being embedded or pre-programmed in customer smart cards and also committed to secure split key escrow databases, furthermore, split cryptographic keys are split key escrowed by party s's, minimal of 2 count of sole split key escrow parties en, also having no knowledge of customer identifications [ID's], furthermore, pre-programmed smart cards are passed from party g, to trusted system s's, smart card distribution party d, having knowledge of customer identification's [ID's] while having absolutely no knowledge of whole cryptographic keys, furthermore, party d further distributes said smart card format, securely distributed to said middle cryptography layer's, commercial industry group customers while also party d, has computer database registered said industry customers in its own industry customer identification [ID] database,

whereby this process claim has achieved, that system party s's said whole key generation party g, has generated by this process whole cryptographic customer keys while having 0% knowledge of customer identifications [ID's], furthermore, party s through its key generation party g, has distributed said whole cryptographic keys, always securely contained inside of said smart cards' provided, said

tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], to party s's, system distribution party d, having 100% knowledge of customer identifications [ID's] and 0% knowledge of whole system cryptographic keys, furthermore, system party g has created said whole cryptographic keys, stored inside of provided, said permanent memory, of provided said computer relational databases, therein being stored inside of split key system databases, furthermore, assuming said smart card non-volatile, memory capacity increases and inversely proportional, device cost decreases, over the coming only few years with semi-conductor device physics very high probability, only assuming Moore's Law rule of thumb of industrial engineering planning, of exponentially doubling semi-conductor individual IC device capacity every 22 months, into at least a few more future years.

68. (NEW) The invention and processes of claim 66 whereby the process step of generating of a set of unique per vendor, commonly distributed only in provided, said tamper resistant hardware [TNV-EEPROM], media distribution vendor cryptographic keys eventually used in a provided, said prior art, and also a provided, said new art, cryptographic digital signal processor [C-DSP] structural means, involving several processes with a 1st example being a, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, being structural means exampled by the, prior art, popular Texas Instrument's TMS-320 digital signal processor [DSP], along with fictional, easily added by modern silicon compiler library methods, additional silicon compiler designed functions for the US Federal National Institute for Standards and Technology's [NIST's] Clipper-Capstone chip, having structural means of embedded tamper resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], furthermore, a 2nd example means being said, new art cryptographic digital signal processor [C-DSP] structural means, being a new art, digital signal processor [DSP] such as the easily supplemented, prior art, Texas Instruments TMS-320, having additional silicon compiler designed functions for prior art algorithm means for subsequent customer uses of digital signal compression audio-video digital compression means involving several processes and components with first example audio-video digital compression means involving several processes being given as prior art, Moving Picture Electronics Group standards X [MPEG X], second example audio-video

digital compression means being given as prior art, fast wavelet audio-video compression or convolutional coding compression, 3rd example structural means, being audio only digital compression means, being given as prior art, MPEG 1 audio layer 3 [MP3], and 4th example structural means of audio only digital compression means being given as prior art, fast wavelet audio only compression [advanced audio CODEC or AAC], furthermore, with subsequent customer uses of a prior art, pass-thru encryption means involving several processes and components which are used to transfer said unique customer cryptographic keys over wiretapable or open computer buses ('red buses') with a first example pass-thru encryption means given as common, family key, secret key encryption, a second example pass-thru encryption means given as common family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor public keys followed by the relevant vendor public key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor public keys followed by relevant vendor private key decryption of the received data block, and a third example pass-thru encryption means being a family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor secret keys followed by the relevant vendor secret key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor secret keys followed by relevant vendor secret key decryption, for eventual manufacturing

into a cryptographic media player, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party G, using prior art algorithms for both public key and secret key cryptography to generate a unique set of vendor cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding in entirety, said unique set of vendor cryptographic keys in an organizational table form means involving several processes with first example organizational table form means being a unique vendor system key table which is indexed by a vendor identification number, furthermore, said organizational table form means is semi-conductor foundry factory embedded into each and every cryptographic digital signal processor [C-DSP] structural means, while specific vendor private keys and vendor secret keys including a minimum count of one vendor key of the private key of vendor party vn, are factory time embedded into each and every one of vendor party vn's eventually distributed media ticket smart cards inside of its embedded cryptographic micro-processor [C-uP] for use in a pass-thru encryption means of several example pass-thru encryption means as explained in a separate process, which is accomplished through the sub-steps of:

generating of vendor secret keys [sek-vn], unique to each media distribution vendor, party Vn, for later use in embedding a complete set of media distributor secret keys [sek-v1 to sek-vn], furthermore, considering that y. 2002 considered secure secret key, secure key bit lengths are from 56-bits excluding parity bits in

triple key modes equivalent to 168-bits up to non-triple key mode use of a secret key length of 256-bits without parity bits with a constant need for key strength increases to counter scalable computer technology improvements, furthermore, programmed internally into every cryptographic media player, along with a system family key [fak-F], and also for eventual indirectly passing out to each media distribution vendor, party vn, only his own secret key [sck-vn],

generating exclusively by party g of unique vendor private key [prk-vn], public key (puk-Vn) pairs, for each media distribution vendor, party vn, for embedding a system family key [fak-F], furthermore, considering that y. 2002 considered secure system key bit lengths are 512-bits for secret key encryption and 3048-bits for public key encryption with adjustments for each type of application with a minimum ten year field use before upgrade assumption requiring an assumed, linear yearly increase in minimum key lengths giving exponential key strength improvements by a power of two, furthermore, a complete set of vendor public keys [puk-V1 to puk-Vn], furthermore, y. 2002 considering that secure public key, secure key bit lengths are from 1024-bits up to 2048-bits with a constant need for linear key length increases to counter constant exponential improvements in computer technology, furthermore, a complete set of vendor private keys [prk-V1 to prk-Vn], furthermore, y. 2003 considered digitally secure at the same bit lengths as the public keys for most public key algorithms, furthermore, in a pre-embedded, common, vendor look-up table form

using an efficient vendor table look-up index to the vendor which is family key encrypted for transit, into each and every provided, said cryptographic digital signal processor [C-DSP] structural means for eventual manufacture into every authorized provided, said cryptographic media player [C-MP] structural means,,

escrowing of split cryptographic keys, exclusively by a minimum of 2 parties en, of all vendor split cryptographic keys, generated with a minimum of 2 central public key escrow authorities, parties en, and other split key escrow, minimum of 2 parties en actions,

whereby this process claim has achieved, a highly federated cryptographic system architecture's only top-most layer is implemented by using: secret secure whole cryptographic system keys being secretly centrally generated by trusted system party s's, sole key generation party g, having knowledge of whole cryptographic keys but absolutely no knowledge of customer identifications [ID's], while also by party g being embedded or pre-programmed in customer smart cards and also committed to secure split key escrow databases, furthermore, split cryptographic keys are split key escrowed by party s's, minimal of 2 count of sole split key escrow parties en, also having no knowledge of customer identifications [ID's], furthermore, pre-programmed smart cards are passed from party g to trusted system s's, smart card distribution party d, having knowledge of customer identification's [ID's] while having absolutely no knowledge of whole cryptographic keys, furthermore, party d further distributes said

smart card format, securely distributed to said middle cryptography layer's, commercial industry group customers while also party d, has computer database registered said industry customers in its own industry customer identification [ID] database,

whereby this process claim has achieved system party s's said whole key generation party g, has generated whole cryptographic customer keys while having 0% knowledge of customer identifications [ID's], furthermore, party s has distributed said whole cryptographic keys securely contained inside of said smart cards' said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM] to system distribution party d, having 100% knowledge of customer identifications [ID's] and 0% knowledge of whole system cryptographic keys, furthermore, system party g has created said whole cryptographic keys, stored inside of provided said permanent memory, of provided said computer relational databases, therein being stored inside of split key system databases, furthermore, assuming provided, said smart card's non-volatile, memory capacity increases and inversely proportional, device cost decreases, with very high probability over the coming few years, through the application of semi-conductor device physics Moore's Law [G. Moore], rule of thumb of industrial engineering planning, of exponentially doubling semi-conductor individual IC device capacity every 22 months.

69. (NEW) The invention and processes of claim 66 whereby the process or methods steps of generating of a unique media ticket smart card cryptographic key set or also known as a unique customer party a's cryptography key set, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using prior art algorithms for both public key and secret key cryptography to generate unique customer cryptographic keys, while having absolutely no access to customer identifications, furthermore, the sub-process of embedding into a single provided, said unique media ticket smart card a unique customer party a's cryptographic key into its provided, said cryptographic micro-controller [C-u-CTLR], which is accomplished through the sub-steps of:

generating of public key pairs for different customers, parties a, b, c, i to z, comprising of private keys (prk-n) and corresponding public keys (puk-n), while having absolutely no access to customer identifications and using prior art public key cryptography,

generating of an incremented, top secret customer index number [CIN], also a related publicly published, message authentication cipher [MAC] taken of the said, public citizen identification number [CIN] or [MAC(CIN)], furthermore, assuming for publicly global Internet-Web publishing as a customer ID number, said

[MAC[CIN]], a future assumption of no distributed system party s's, central cryptographic system keys and thus being deliberately used backwards from the traditional public and private use ordering of some previous cryptographic architectures, furthermore, composed of the structural means of ~~the message authentication cipher [MAC], which is a secret~~ initialization vector [IV] based, message digest cipher [MDC], of customer index number [MAC[CIN]], which is publicly printed upon the exterior of each media ticket smart card as a non-anonymous, public customer identification [ID],

generating of a global Internet-Web published list of public customer identification numbers [ID's], furthermore, comprising of a customer provided said, prior art, public key relational database [RDB], furthermore, which indexes a message authentication cipher [MAC] taken of any given, customer party a's, out of parties: a, b, c, i to z, index number [MAC[CIN]], ~~having a provided said, prior art, relational database's [RDB],~~ blank or no entered value, private key field, to the corresponding public key for any given customer a, said relational database being passed back to the central public key distribution authority, party d,

embedding into media ticket smart card a, a means for pass-thru encryption with 1st example pass-thru encryption means being a single, common, system family key [fak-F], furthermore, known as being vulnerable to a single point hacker attack to breach the entire system, and 2nd example pass-thru encryption means

being a complete pre-embedded, common, vendor public and private key table which is accessed with a vendor index; furthermore, the private key [prk-a] for unique customer party a, indexed by message authentication cipher [MAC] of customer index number [MAC[CIN]] also known as the public customer identification number, also

embedding into media ticket smart card b, a system family key [fak-F], the private key [prk-b] for customer party b indexed by message authentication cipher [mac] code of customer index number [MAC[CIN]], etc.,

generating of an initial provided, said media ticket smart card's access code structural means; involving several processes and components such as a 1st access code means of a unique password, a 2nd access code means of a unique passphrase-passcode, a 3rd access code means of a unique bio-identification, with storage into a common database organizational means involving several processes and components with first example common database organizational means being a data structure indexed by message authentication code [mac] of customer index number [MAC[CIN]] for release to the central public key escrow, access code authority, party el, who will later on release it to the registered customer for initial media ticket smart card use,

handing the provided; said media ticket smart cards; to the public key distribution authority, party d, and furthermore,

escrowing of all customer split cryptographic keys generated with a minimum of 2 central public key escrow authorities, parties en, and other escrow actions,

whereby this process claim has implemented a highly federated cryptographic system architecture's only top-most layer is implemented by using: secret secure whole cryptographic system key being secretly centrally generated by trusted system party s's, sole key generation party g, having knowledge of whole cryptographic keys but absolutely no knowledge of customer identifications [ID's], while also by party g being embedded or pre-programmed in customer smart cards and also committed to secure split key escrow databases, furthermore, split cryptographic keys are split key escrowed by party s's, minimal of 2 count of sole split key escrow parties en, also having no knowledge of customer identifications [ID's], furthermore, pre-programmed smart cards are passed from party g to trusted system s's, smart card distribution party d, having knowledge of customer identification's [ID's] while having absolutely no knowledge of whole cryptographic keys, furthermore, party d further distributes said smart card format, securely distributed to said middle cryptography layer's, commercial industry group customers while also party d, has computer database registered said industry customers in its own industry customer identification [ID] database,

whereby this process claim has achieved a system party s's said whole key generation party g, has generated whole cryptographic

customer keys while having 0% knowledge of customer identifications [ID's], furthermore, party s has distributed said whole cryptographic keys securely contained inside of said smart cards' said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM] to system distribution party d, having 100% knowledge of customer identifications [ID's] and 0% knowledge of whole system cryptographic keys, furthermore, system party q has created said whole cryptographic keys, stored inside of provided said permanent memory, of provided said computer relational databases, therein being stored inside of split key system databases, furthermore, assuming said smart card non-volatile, memory capacity increases and inversely proportional, device cost decreases, over the coming only few years with semi-conductor device physics very high probability, only assuming Moore's Law rule of thumb of industrial engineering planning, of exponentially doubling semi-conductor individual IC device capacity every 22 months, into at least a few more future years.

70. (NEW). The invention and processes of claim 66 whereby the process or method or steps to do distributing of provided, said cryptographic digital signal processors [C-DSP's] structural means, is based upon the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing provided, said cryptographic digital signal processors [C-DSP's] structural means, to media distribution vendors, for manufacturing into provided, said cryptographic media players [C-MP] structural means,, furthermore, while being assumed to have by legal law and administrative rule means, absolutely no access to whole cryptographic keys, which consists of the sub-steps of:

distributing of the provided, said cryptographic digital signal processors [C-DSP's] structural means, in a physically secure transport and audit trailed chain of control by the central public key distribution authority, party d, only to authorized media distribution vendors, parties vn,

manufacturing by the authorized media distribution vendors, parties vn, of the provided, said cryptographic digital signal processor [C-DSP] structural means, into different forms of provided, said cryptographic media players [C-MP] structural means,, with various specialized functions and applications tailored to specific market applications and marketing price-points,

retailing by the authorized media distribution vendors of provided, said cryptographic media players [C-MP] structural means,, each having a vendor unique, embedded provided, said cryptographic digital signal processor [C-DSP] structural means, with various specialized functions and applications to consumers,

whereby this process claim has achieved, a said party s, having said whole key distribution party d, who has been given 0% whole key knowledge, but, 100% knowledge of customer identifications [ID's], who has been administrator of provided, said cryptographic digital signal processor [C-DSP] structural means' hardware distribution process, which has enabled only trusted national commercial, cryptographic hardware vendors who are legally allowed by party d, to firmware program with confidential system cryptographic keys, provided, said tamper resistant non-volatile memory [TNV-EEPROM] internal to each provided, said cryptographic digital signal processor [C-DSP] structural means, in order to keep said system keys top secret, furthermore, at the middle level layer of cryptographic system hardware's world-wide distribution chain, under administration of said party d, said PC cryptographic hardware plug-in board classes of hardware vendors, are simply given by said system authority distribution party d, 100% pre-programmed with cryptographic system keys, provided said, tamper resistant non-volatile memory [TNV-EEPROM], which is pre-stored internal to centrally distributed, provided, said cryptographic digital signal processor [C-DSP] structural means, and also provided, said cryptographic integrated circuit device classes [C-

IC's], used to install in their PC peripheral device hardware, furthermore, at the middle cryptographic layer of said party d administered, digital media distribution vendor parties vn, the cryptographic layer of commercial system administrators having vested commercial interests with their own commercial industry groups, furthermore, desirably aided in commercial secrets enforcement by future, commercial anti-espionage felony laws, furthermore, at the said parties vn administered, bottom cryptographic architecture layer of said customer and his unique per customer, only said smart card distributed and securely protected by provided, said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], cryptographic keys, are known only to the highly federated middle vendor or key industry layers of commercial, split key escrow databases, altogether implementing a highly federated cryptography system.

71. (NEW) The invention and processes of claim 66 whereby the process of steps to do distributing of the provided, said media ticket smart cards, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party D, distributing unique to each customer, cryptographically programmed, provided, said media ticket smart cards, to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys, which consists of the sub-steps of:

assigning of provided, said media ticket smart cards, eventually to media ticket smart card users or individual customer parties: a, b, c, i to z, which is the sub-step done by the central public key distribution authority, party d, assigning media ticket smart cards received from the public key generating authority from the methods of process step 69, to authorized media distribution vendors and eventually to media ticket smart card customers who will register names, addresses, etc. which can be mapped into a prior art, provided, said relational database [RDB], by the publicly known message authentication cipher [MAC], of unique, public information, customer index number [MAC[CIN]], furthermore, being printed for external provided, said media ticket smart card public identification, on the exterior of the provided, said media ticket smart card,

imprinting of provided, said media ticket smart cards which is the sub-step done by the central public key distribution authority, party d, imprinting the provided, said media ticket smart cards with customer identification which fields are accessed by using the media ticket smart card customer identification field family key obtained from the public key generating authority,

distributing of provided, said media ticket smart cards to the customer parties: a, b, c, i to z, which is the sub-step done by the central public key distribution authority, party d, giving the provided, said media ticket smart cards to authorized media distribution vendors, parties vn, for selling the provided, said media ticket smart cards to media ticket smart card customers parties: a, b, c, i to z, through an appropriate secure physical channel such a retail store, express mail, and registered mail which provided, said media ticket smart cards, are useless without registration with the central public key distribution authority, party d, and receiving of a temporary media ticket smart card access codes or temporary activation codes, unless an optional, wildcard access code was programmed by the public key generating authority,

possessing of provided, said media ticket smart cards, which is the sub-step done by the customer, party a, receiving a media ticket smart card with exterior message authentication code [MAC] of the relevant, customer index number [MAC[CIN]] and registering the media ticket smart card at the retail store or by mailing back in a registration card with customer party's: party a, b, c, i to z's, individual customer identification [customer ID]: name, address,

phone number, e-mail address, etc., and public customer identification number, which will allow the central public key distribution authority, party d, to use its customer database to map such identifications to the customer's public key,

publishing of the public keys which is the sub-step done by the central public key distribution authority, party d, openly publishing using provided, said internet protocol [IP], over the global internet from a web server, Web publishing all public keys and appropriate user identities [ID's], such as name and message authentication cipher [MAC] of customer index number [[MAC[CIN]], with a publishing example means using several process steps being the widely used, industry standards committee established, International Telegraphy Union's [ITU's] X.509 digital certificate format,

handling of media ticket smart card temporary user access codes which is the sub-step done by the central public key distribution authority, party d, handing only customer name, mailing address, and phone number indexed by a unique customer identification means involving several processes with a first unique customer identification means being a message authentication cipher [MAC] of the secret customer index number [CIN], to said public key escrow, access code authority [puk-e1] which said public key escrow, access code authority party [puk-e1], already has from process 69, the media ticket smart card temporary access codes also indexed by the same message authentication cipher [MAC] of the secret customer index number [CIN], furthermore, the public key escrow, access code

authority party [puk-e1], has no media ticket smart cards or media ticket smart card reader family key from process 67,

distributing of media ticket smart card temporary user access codes, which is the sub-step done by said public key escrow, access code authority, party e1, matching customer names, mailing address, and phone number to temporary media ticket smart card access codes in order to mail out media ticket smart card temporary access codes to media ticket smart card users, after which the public key access code authority promptly destroys all information it has used except for confirmation of the mailing,

whereby this process claim has achieved, a distributed, uniquely programmed, provided, said media ticket smart cards and then distributed them in a commercial cryptographically secure manner, out to the customer parties: a, b, c, i to z, while not exposing to any hacker party h, any unique to customer parties: a , b, c, i to z, whole private keys or whole secret keys.

72. (NEW) The invention and processes of claim 66 whereby the process of steps to do escrowing of the split cryptographic keys which is the process done by the central public key generation authority, party g, safe-guarding the split cryptographic customer keys, and split cryptographic vendor keys in an entirely secure and confidential manner with legal 1st means for simple customer identification and lost key recovery, 2nd means for disputed ownership court ordered recovery, and 3rd means for court ordered only use by law enforcement, which is accomplished through the sub-steps of:

receiving of the split cryptographic customer key programmed, prior art, provided, said relational database [RDB] of customer private keys, PrK-n or a minimum of a front half and a back half key, and also the split cryptographic vendor key database of vendor private keys, prk-vn, and vendor secret keys, sek-vn or a minimum of a front half and a back half key, which is the sub-step done by the central public key escrow authorities, parties en, receiving split key databases from the central public key generation authority, party g,

anti-collaborating prevention means which is keeping separate the key split customer and vendor cryptographic keys between a minimum of two, for a front half of key and a back half of key, independent key escrow authorities, parties en, who have absolutely no access to customer identifications,

receiving of provided, said media ticket smart card owner customer party's a out of customer parties: a, b, c, i to z, initial media ticket smart card access codes or activation codes, which is the sub-step done by the independent public key access code authority, party e1, receiving from the public key generation authority, party g, a database of initial media ticket smart card access codes, all commonly indexed by message authentication cipher [MAC] of customer index number ([MAC[CIN]] and also receiving from the central public key distribution authority, party d, customer identifications [ID's]: customer names, mailing addresses, and e-mail accounts also indexed by message authentication cipher [MAC] of customer index number ([MAC[CIN]],

distributing of media ticket smart card initial access code or activation code structural means, involving several processes and components with 1st example access code means being a unique password, and 2nd example access code means being a unique pass phrase or pass code, and 3rd example access code means being unique bio-identification which must be 'warm-blooded' authorized human agent programmed into the smart card after 'warm-blooded' human customer authentication, and 4th and the highest security access code structural means, being a particular type of two-phase authentication means which involves both bio-identification authentication which must be 'warm-blooded' authorized human agent programmed into said media ticket smart card for bio-identification access code means retrieval along with initial default and subsequent unique customer passphrase-passcode programmed into

provided, said media ticket smart card, for passphrase-passcode access code means done in addition, which is the sub-step done by the public key access code authority, party e1, secure means transmitting through 1st example means of certified mailing or secure e-mailing to customers of the initial access codes, after which receiving back confirmation it promptly destroys all knowledge of customer identifications,

whereby this process claim has achieved said split cryptographic keys are split key escrowed by party s's, minimal of 2 count of split key escrow parties en, also having no knowledge of customer identifications [ID's].

73. (NEW) The invention and processes of claim 66 whereby the process of steps to do layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with a minimum of three layers of digital computer architecture: a highest layer of both cryptography and logic abstraction, bottom-most patent drawing layer, composed of the media ticket smart card system authority, a middle patent drawing layer, composed of authorized media distribution company parties vn, also combining for this process claim, the 2 drawing layers of the hardware vendor parties vn, with the digital media distribution vendor parties vn of the relevant patent drawing, and a top-most patent drawing layer, lowest cryptography and logic abstraction, user layer composed of customers, through the sub-steps of:

layering into a minimum of 3-layers of a federated architecture of cryptographic authority:

a relevant patent drawing's bottom-most layer or centralized layer, composed of a media ticket smart card system authority, party s,

a relevant patent drawing's middle 2 layers, or intermediate layers, composed of authorized media distribution companies vn, furthermore, patent drawing viewed as having 2 sub-layers: a slightly higher sub-layer of system party s's,

whole key generation party g, pre-programmed, cryptographic hardware distribution vendors distributing provided, said cryptographic media players [C-MP] structural means,, and also a slightly lower sub-layer of pre-programmed, provided, said media ticket smart card vendors, and

a relevant patent drawing's, top-most, user layer composed of customer parties: a, b, c, i to z,

whereby this process claim has achieved a highly federated or regional cryptography architecture of a minimal 3 cryptography process claims layers is created which are logically mapped to the relevant patent drawing's 4 of 4 drawing layers by condensing the middle-most 2 drawing layers: claims layer 1: being the said system party s's, bottom-most relevant, patent drawing, cryptography layer of highest cryptographic and logic abstraction, claims layer 2: being the said media distribution vendor parties vn cryptography layer, being the relevant patent drawings 2 middle drawing layers, and claims layer 3: being the said customer parties: a, b, c, i to z, top-most relevant, patent drawing layer, being the lowest cryptography layer or lowest logic abstraction layer.

74. (NEW) The invention and processes of claim 66 whereby the process of steps to do preparing of a unique play code or custom encrypted session key, and also a unique play count or a custom encrypted re-play counts, which is the process done by the authorized digital media distribution company, party vn, preparing said unique play code, a session key or one-time use secret key, and said unique play counts, a paid for number of plays or count of free trial plays, and preparing of the custom encrypted digital media for using provided algorithms for Web custom encrypted media downloading to each customer, through the sub-steps of:

preparing of the media header for each download media session which is:

unique vendor and customer encrypted play code with media header (and sequence numbers):

{

public vendor identification number [MAC[VIN]] = message authentication cipher [MAC] of top secret vendor index number [vin],

session identification number,

customer party a, public key encrypted{

vendor secret key encrypted{

vendor digitally signed {play code

(session key or one-time secret key),

vendor sequence number,

message authentication cipher [MAC]

of customer identification number

[MAC[CIN]]})),

customer (pass-thru encryption use) sequence number,

} = temp-9a,

unique vendor and customer encrypted play count with media header [and sequence numbers]:

{

public vendor identification number [MAC[VIN]] =

message authentication cipher [MAC] of top secret vendor index number [VIN],

session identification number,

customer A public key encrypted{

vendor secret key encrypted{

vendor digitally signed {play count

{paid for numbers of plays,

-1 for infinite plays,

count of free trial plays),

vendor sequence number,

message authentication cipher [MAC]

of customer identification number

[MAC[CIN]}})),

customer (pass-thru encryption use) sequence number,

} = temp-9b,

encrypting of the play codes or session keys or one-time use only, secret keys, which are truly random numbers in a desired range with header is a process of first, the vendor digitally signs [prk-vn] the decrypted play code, and then attaches the header and sequence number and secondly, the vendor three-way encrypts the result with the sequence of first encryption with the secret key of the vendor, sek-vn, second encryption, with the public key of receiving customer, party a, puK-a, third encryption with the system family key, fak-F, for pass-thru encryption means with first example pass-thru

encryption means being common family key encryption or a known single point of vulnerability if breached:

Vn-fak-F[temp-9a]

= pass-thru encrypted play code with header, and sequence numbers,

which first pass-thru encryption means requires for pass-thru decryption on the receiving end, the common family key symmetric cryptography based decryption in an exactly similar manner,

second pass-thru encryption example means being using the public key of the transmitting end vendor, puk-vn, with a pre-embedded, common, vendor private and public key table efficiently accessing by the receiving end vendor, party vn', with use of a table index which is family key encrypted to avoid tampering:

{vn-fak-f (index to the vendor key table), vn-puk-vn(temp-9a)}

= pass-thru encrypted play code with header (and sequence numbers),

which second means of pass-thru decryption requires for pass-thru decryption both the common family key, vn'-fak-f, and the unique vendor private key, vn'-prk-vn,

third pass-thru encryption example means being the transmitting vendor, party vn, using the transmitting vendor's unique secret key,

seK-vN, and a family key encrypted table index to a pre-embedded, common table of unique, secret vendor keys in:

{vn-fak-f (index to the vendor secret key table),

vn-sek-vn (temp-9a)}

= pass-thru encrypted play code with header (and sequence numbers),

which third pass-thru encryption means requires for pass-thru decryption both the common family key, vn'-fak-f, and the unique vendor secret key, vn'-sek-vn,

furthermore:

in the given in this system usual absence of an authorized and trusted system wide, synchronized system of clocks used with a time-stamping technique, the alternate method of sequence number use is needed to prevent 'recorded replay hacker attacks' or digital recordings of encrypted messages and complete digital re-plays in entirety without decryption, on wiretapable buses of pass-thru encrypted signals inside of the cryptographic media player, furthermore, the sequence number can only be incremented by a party with the vendor secret key [sek-vn], customer private key [prk-n], and system family key [fak-f] who are the party g, for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party p, for any vendor which player has

a collection of all vendor secret keys [sek-v1 to vn] and a collection of all vendor private keys [prk-v1 to vn], furthermore, used in key ownership re-assignment operations by the cryptographic digital signal processor [C-DSP] structural means in the cryptographic media player, party p, furthermore, the customer's family key, sequence number is used in media ticket smart card loop-back operations, furthermore, the player can also check the vendor digital signature, and can obtain the customer party a's private key [prk-a] and public key [puk-a] from customer's inserted media ticket smart card a,

encrypting of play counts (counts of paid for numbers of play, 1 binary encoded for indefinite plays, or to binary N counts, of free trial plays, furthermore, which are encrypted by the sequence of using the first example pass-thru encryption means using the common family key [fak-f] which is known vulnerable to breaches:

vn-fak-vn(temp-9b)

= pass-thru encrypted play count with header, and sequence numbers,

with the second example pass-thru encryption means using the vendor public key being obvious from the above example in this same claim, and third example pass-thru encryption means using the vendor secret key also obvious from the above example in this same ~~claim~~ process step,

whereby this patent process claim has achieved, said play code or custom encrypted session key, and said play count or custom encrypted re-play counts, implemented by said play codes, of highly commercial vendor controlled custom cipher text digital media, prior art, provided, said global Internet-Web published to targeted said customer parties a, b, c, i to z, distribution of digital media, furthermore, allowing unlimited 'digital to digital' copying of generated digital media in output, custom cipher text format, without impeding the existing digital computer industry in any way, while at the same time not impeding in any way the format of non-cipher text format digital media, furthermore, for a private digital media owner desiring of privacy in limited controlled distributions, pre-configurable controls of the digital media, has been implemented by the methods of this process, said play count controlled re-plays, or count controlled re-plays, only exampled by 10 free trial sample digital media plays before automatic digital media deactivation, exampled by 10 low-cost trial sample digital media plays of new music or new movies, before charging a higher cost, exampled by 1,000 paid for digital media plays before forcing a paid subscription renewal order,

whereby this patent process claim has achieved, said custom encrypted digital media or custom cipher text digital media format, created by this invention's present process, can be digital to digital copied ad infinitum by digital PC computer equipment, being of little use to the both legal copier party z, and also of little use to the illegal or non-authorized, international copyright copier being designated, hacker

party h, without the related smart card stored custom said play codes and said play counts, furthermore, enabling a method under US Copyright law, partial legal fair use, archival duplication only of physical permanent memory custom cipher text media, in case of fires, flood, mud slides, tornadoes, hurricanes, outside theft, employee theft and assorted disasters.

75. (NEW) The invention and processes of claim 66 whereby the process of steps to do downloading to customer, party a, at a private dwelling, prior art, insecure ['red bus'], personal computer (PC) which is the process done by the authorized digital media distribution vendor, party vn, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a centralized, digital media distribution authority, hosted on a provided, world wide web [WWW] server over the provided, global Internet to prior art, provided, multiple personal computer [PC] based web clients of encrypted play codes or one-time secret keys or session keys, with header and encrypted play counts or paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into media ticket smart cards attached to personal computer media ticket smart card readers, and one-way transfer of custom session key or one-time use only secret key encrypted digital media which is pre-unique vendor secret key encrypted, for deposit into physical digital media inserted into media drives attached to personal computers, through the sub-steps of:

encrypting for Web download from a trusted Web system server to the media ticket smart card in a personal computer [PC] using pass-thru encryption means involving several processes and components for transferring any type of pre-vendor unique secret key encrypted and sequence numbered digital data securely from any trusted Web server system source, over the wiretapable ['red bus'] Internet,

down to any trusted media ticket smart card inserted into a prior art personal computer [PC], with a 1st example pass-thru encrypting means being said common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, a 2nd example pass-thru encrypting means being a single unique originating vendor private key digital signaturing into 'signatured text (non-encrypted and readable by anybody)' and then the answer vendor's unique public key used for public key encryption on the trusted Web server assuming that the media ticket smart cards each have an entire common, embedded set of a unique vendor look-up table of both vendor public keys and vendor private keys with first organizational means involving several processes and components being a row and column look-up table indexed by unique vendor identification number, a 3rd example pass-thru encrypting means being a unique vendor secret key used for secret key encryption, combined with secret key signaturing, on the trusted Web server assuming that the media ticket smart cards each have an entire common, embedded set of a unique vendor look-up table of unique vendor secret keys with first organizational means being a row, column table indexed by a vendor identification number,

encrypting for Web upload from a media ticket smart card in a personal computer [PC] to a trusted Web system server using pass-thru encrypting return means involving several processes and components for transferring any type of closed-loop, feed-back path digital data securely from a trusted system destination from a trusted media ticket smart card inserted into a personal computer

[PC] over the wiretapable ['red bus'] Internet back to the trusted Web server, with a 1st example pass-thru encrypting return means being said common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, a 2nd example pass-thru encrypting return means assuming that each media ticket smart card has an entire common, embedded, said look-up table of unique vendor public keys and private keys, being an answer vendor's private key digital signaturing to signatured text or non-encrypted text thus readable by any party, followed by the unique originating vendor's public key for public key encryption to 'cipher-text' or encrypted text with use of the pre-embedded in each media ticket smart card, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being the row, column table indexed by a vendor identification number, a 3rd example pass-thru encrypting return means being said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being the row, column table indexed by a vendor identification number,

accounting by credit card if payment for the custom encrypted digital media is due to the media distribution vendor,

cryptographing from a media distribution vendor's secure media web server to a customer party a's personal computer [PC] using prior art, commercial, low security, secure sockets layer [SSL] hybrid key cryptography of already pass-thru encrypted with

incremented sequence numbers used to prevent recorded replay attacks, encrypted play codes, one-time secret keys or session keys, with header and encrypted play counts, paid for counts of plays or decryptions or else counts of free trial plays, with header for deposit into media ticket smart cards attached to built-in media ticket smart card readers,

cryptographing from a media distribution vendor's secure media web server to a customer party a's personal computer [PC] using prior art, commercial, low security, secure sockets layer [SSL] hybrid key cryptography of already custom, encrypted digital media for deposit into physical media inserted into built-in media drives,

whereby this process claim has achieved, a middle cryptographic 1 of 3 claims layers or relevant patent drawings combined 2 of 4 middle drawing layers, broadened for process claims purposes, when the 4 process claims layers are logically mapped to the relevant patent drawings 4 of 4 drawing layers: of relevant patent drawing's 1 of 4 bottom drawing layers of said party d administered, of 2 of 4 middle drawing layers or 1 middle claims layer, digital media distribution vendor parties vn, the cryptographic claims layer of commercial system administrators having vested commercial interests with their own commercial industry groups, furthermore, at the said parties vn administered, top-most cryptographic architecture claims layer or relevant patent drawing's 1 of 4 top-most drawing layer, of said given

customer party a, out of customer parties: a, b, c, i to z, and his unique per customer party a's, only said smart card a, distributed and securely protected by provided, said prior art, tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], cryptographic keys, are known only to the highly federated middle claims layer vendor parties, or relevant patent drawing's 2 of 4 middle drawing layers, being key industry layers of commercial, split key escrow databases, alltogether implementing a highly federated cryptography system.

76. (NEW) The invention and processes of claim 66 whereby the process of steps to do delivering by foot which is the process done by the given customer, party a, done to both: physical custom encrypted digital media belong to the given customer party a, also the given customer party a's, programmed by process claim 75, provided, said media ticket smart cards, process of being physically transferred from the given customer party a's, provided, said prior art, personal computer [PC] structural means which can be for security reasons be an up-graded provided, said cryptographic personal computer [C-PC] structural means, to any other customer party's provided, said cryptographic media player [C-MP] structural means, having a built-in, provided, said media ticket smart card reader, which consists of the sub-steps of:

transporting his own custom encrypted digital media to any provided, said new art, cryptographic media player [C-MP] structural means,, along with his own provided, said media ticket smart card a, with a 1st example means being a given customer a, foot-step transfer, and a 2nd example means being a provided, said, digital serial computer link used to non-secretly or non-privately, electronically transfer custom encrypted cipher text between provided, said prior art, non-volatile memory,

inserting of his own custom encrypted digital media and his own provided, said media ticket smart card a, into any provided, said cryptographic media player [C-MP] structural means, with a built-in, provided, said media ticket smart card reader,

whereby this process claim has achieved, a top-most or least abstracted, cryptographic system architecture claims layer, mapped for process claims broadening purposes, to the relevant patent drawing's top-most 1 of 4 drawing layers, of the individual commercial customer drawing layer, the said individual customer parties: a, b, c, i to z, having by previous process claims downloaded both the custom cipher text digital media and the corresponding play codes or encrypted 1-time use only secret keys or session keys, and play counts or encrypted count controlled plays, has by this process claim physically transferred means, the provided said, permanent digital computer memory storage device structural means, in some cases being physical transfer of removable memory modules are removed from the download device, and inserted into a provided, said cryptographic media player [C-MP] structural means,, or in additional cases being a physical, secure, provided, said digital serial data link, connecting permanently installed computer memories on both ends for custom encrypted cipher text transfer, with the also required and completed by this process claim, physical transfer means of the matching provided, said prior art, media ticket smart card, which is the given smart card a, given customer party a, removed from download device provided, said prior art PC and provided, said new art cryptographic PC [C-PC], and customer

party a inserted, into provided said, cryptographic media player [C-MP] structural means.

77. (NEW) The invention of claim 66 whereby the process of steps to do said encrypting in a pass-thru means which involves several other processes for media ticket smart card upload to provided said cryptographic media player having an embedded, provided said cryptographic digital signal processor (C-DSP) means using pass-thru encrypting means involving several processes and components for transferring any type of digital data securely from originating said media ticket smart card up to answering said cryptographic digital signal processor (C-DSP) means, with a 1st example pass-thru encrypting means being said common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, a 2nd example pass-thru encrypting means being originate vendor, unique, vendor private key digital signaturing to 'signatured-text (not encrypted text thus readable by any party)' followed by answering vendor, unique, vendor public key digital public key encryption to 'cipher-text (encrypted text)' using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being a row, column table indexed by a vendor identification number, a 3rd example pass-thru encrypting means being originate vendor, unique, vendor secret key encryption to 'cipher-text (encrypted text which combines signaturing)' using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving

several processes and components with first organizational means being a row, column table indexed by a vendor identification number,

whereby this process claim has achieved, cryptographic data which has been structurally protected from open or wiretapable digital computer buses, hacker party h, wiretapping efforts, by any number of structural means of above stated efforts, having many prior art well known alternate structural means of a similar functional means.

78. (NEW) The invention of claim 66 whereby the process of steps to do said encrypting in a pass-thru return means for said cryptographic media player's embedded said cryptographic digital signal processor (C-DSP) means download to said media ticket smart card using pass-thru encrypting return means involving several processes and components for transferring any type of digital data securely from said cryptographic digital signal processor (C-DSP) means to said media ticket smart card with a 1st example pass-thru encrypting return means being common family key or shared secret key encryption which is known vulnerable to a single point of failure, 2nd example pass-thru encrypting return means being answer vendor unique private key digital signaturing to 'signatured-text (non-encrypted thus readable by any party)' followed by originate vendor unique public key encryption to 'cipher-text (encrypted text)' using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being the row, column table indexed by a vendor identification number, a 3rd example pass-thru encrypting return means being answer vendor unique secret key encryption to 'cipher-text (encrypted text which combines signaturing)' using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being the row, column table indexed by a vendor identification number,

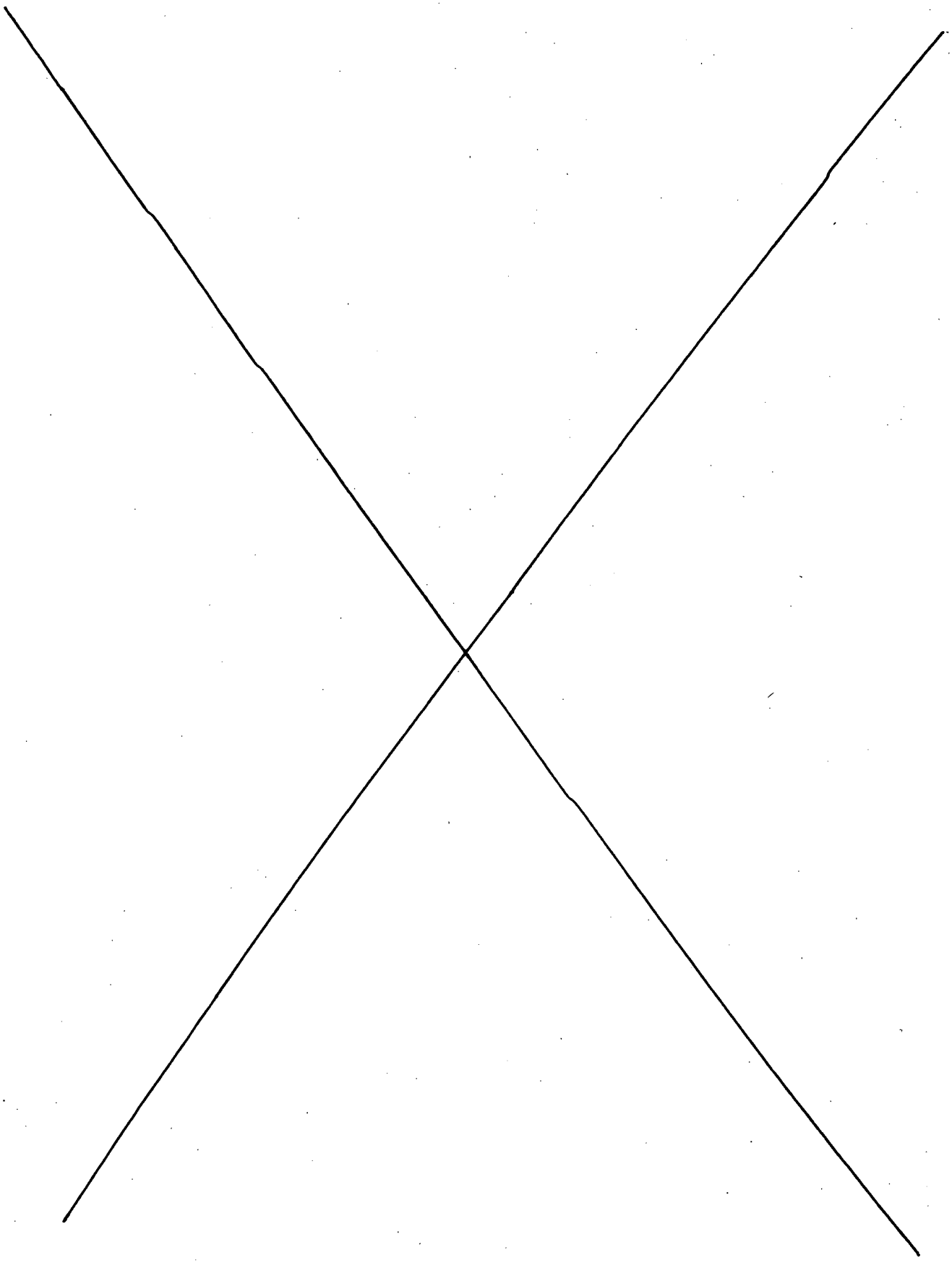
whereby this process claim has achieved, cryptographic data which has been structurally protected from open or wiretapable digital computer buses, hacker party h, wiretapping efforts, by any number of structural means of above stated efforts, having many prior art well known alternate structural means of a similar functional means.

79. (NEW) The invention and processes of claim 66 whereby the process of steps to do initializing before playing which is the process done by the given, customer, party a, out of parties: a, b, c, i to z, of preparing any customer party's: a, b, c, i to z's, provided, said new art, cryptographic media player [C-MP] structural means, with its contained, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, by inserting his own given party a's, unique custom encrypted digital media, and also by inserting his own given party a's, unique media ticket smart card a, comprising of the sub-steps of:

verifying of insertion by some customer of custom session key (one-time secret key) encrypted media of the process of independent claim 66 origins, into the provided, said new art, cryptographic media player's [C-MP] structural means' media drive,

verifying of insertion by some customer of some media ticket smart card A into the built-in media ticket smart card reader on the cryptographic media player,

whereby this process claim has achieved the preparation steps of said cryptographic media player having been completed to prepare for digital media playing.



80. (NEW) The invention and processes of claim 79 identifying of relative high security applications in need of a high degree of authentication of the customer where high security needs are more important than customer extra time and effort, versus relative medium security applications, versus relative low security applications, which comprises the sub-steps of:

assuming of standardized by the process of this patent, industry standard, provided, said new art, smart cards with bio-ID, and containing of provided, said prior art, tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], paired with industry standard provided, said prior art, PC based, said bio-ID smart card readers, supporting of all of standardized bio-ID smart card physical and electrical interface format, relative high security, relative medium-security, and relative low security applications, which are encountered in the field, furthermore, hi-security applications are in need of a mandatory high degree of authentication of the customer, where high security needs are relatively, more important than customer extra time and extra effort,

programming at the factory for a dedicated, high security application, by structural means of pre-programming on the physically protected by hardware, lock and key secure access, building protection, and also digital signatured integrity code

protected, provided, said new art, cryptographic digital media player's [C-MP] structural means, or the machine's dedicated and protected from hackers, built-in firmware using provided, said prior art, electrically erasable programmable read-only memory [EEPROM], by structural means of including a simple, embedded security level, pre-determined binary encoded, digital field code, with functional means for allowing upon firmware start-up or boot-up digital machine execution, absolutely forcing through firmware the structural means setting of a relative high security application level 3 integer value of all specific, hi-security exclusive, provided, said new art, crypto-media player [C-MP] hardware, played digital media application's security level flag, to a pre-determined, integer variable, which is pre-initialized at system start-up time to 0, said flag held in said dynamic random access memory [DRAM], furthermore, said cryptographic media player's [C-MP] structural means, firmware executing of a customer-citizen access code check by using some appropriate security and convenience level means, such as but not limited to dedicated high-security applications such as: government use, banking, credit smart card transactions, debit smart card applications, automatic teller machines [ATM cards], high security facility card key access, US DOD conditional access card use, versus medium and lower security applications of consumer digital media entertainment,

identifying of a relative, low security application, by firstly, having to read said play code from the inserted custom

digital media in order to decrypt said play code, using standard cryptography procedures, thus obtaining the custom encrypted by use of said media distribution vendor created custom said play codes, digital media secure content header, used to determine, relative low security applications with setting of structural means of said unique, digital media application's, media application security level flag to a pre-determined hacker protected, integer 1 value, standing for low security applications, and also relative medium security applications, with setting of said structural means of said digital media application security level flag to a pre-determined hacker protected, integer 2 value, standing for medium-security applications, versus relative high security applications already having its own dedicated setting by claims process 79, furthermore, process claim 79 has already only if relevant for a relative provided, said new art, high security media player structural means, programmed the digital media application security flag to a hacker protected, integer value 3, standing for an exclusive, high security applications, only where customer time and effort is more critical than customer security,

whereby this process claim has achieved a distinguishing by storage of secure memory stored, said media application security level flag, stored inside of a volatile, provided, said prior art, dynamic access random access memory [DRAM], of provided, said new

art, cryptographic digital media player [C-MP] structural means, the relevant security level flag, having allowed execution time or firmware program run-time, distinguishing between: a relatively very high security application, a relatively medium security application, and a relatively low security application.

81. (NEW) The invention and processes of claim 80 whereby the process of steps to do authenticating by customer triangle authentication which is the process done by provided, said new art, cryptographic media player structural means, and its provided said, new art cryptographic digital signal processor [C-DSP] structural means, which process step may be skipped only for relative, low security applications, only when customer time and effort is of essence, accomplished through the sub-steps of:

reading of the structural means of said secure memory, digital media security level flag, which has already been computer programmed through process 80 with a system start up sequence initialization value of integer 0, furthermore, having an execution time value of integer 1 for a relative low-security application, integer value 2 for a relative medium security application, and integer value 3 for a relative high security application,

whereby this process claim has achieved for dedicated relative, high security applications, indicated through program execution of embedded firmware programming of a dedicated, relative high security, provided, said new art, cryptographic digital media player [C-MP] structural means, absolutely has enforced a high security per commercial customer, start-up sequence with subsequent forced reading

of said bio-ID smart card upon every custom cryptographic digital media play.

82. (NEW) The invention or process of 81 whereby the process of steps to do only for relative medium security and also relative high security digital media applications and not for relative low security applications of claim 81 determination by structural means of said digital media security level flag, a process called customer triangle authentication, which is accomplished through the sub-steps of:

transferring media ticket smart card access codes from input/output (I/O) access code entry device means on the cryptographic media player over wiretapable ('red') computer buses to the cryptographic digital signal processor (C-DSP) means with a first example access code means of passphrases/passcodes customer entered into a device entry 1st example means of a built-in cryptographic media player toggle field with a minimum of one-line display, and a 2nd example access code device entry means of being customer entered into a computer keyboard on a personal computer [PC], and a 3rd example access code device entry means of a customer finger entered into a built-in bio-identification [bio-ID] unit such as a digital fingerprint reader, which all example access code device entry means are transferred over provided, said prior art, wiretapable buses ['red buses'] to a provided, said prior art, tamper resistant non-volatile, electrically erasable programmable read-only memory [TNV-EEPROM], and to its containing, provided, said

new art, cryptographic digital signal processing [C-DSP] structural means, which is embedded inside of the provided, said new art, cryptographic media player [C-MP] structural means,

encrypting using pass-thru encryption means of digital data from the media ticket smart card meant for upload to the cryptographic digital signal processor (C-DSP) means with first example pass-thru encryption means being the use of the common and vulnerable, system family key, fak-F, and second example pass-thru encryption means being the pre-stored, unique vendor's private key used with a family key encrypted index to an embedded, common, vendor key look-up table for efficient table look-up which vendor key table pre-stored, on the other end holds the unique, matching public key, for pass-thru encryption by the media ticket smart card of the customer's media ticket smart card access code in 1st example access code means being passphrases/passcodes, and 2nd example access-code means being passwords having automatically mixed in pseudorandom noise called salt, and 3rd example access code means being bio-identification such as a digital fingerprint with an added incremented sequence number with means to avoid recorded replay attacks which is automatically added by the authorized media distribution vendor and the authorized cryptographic media player in order to prevent recorded replay attacks,

transferring using the encrypting using pass-thru encryption means of upload data from the media ticket smart card to the cryptographic digital signal processor (C-DSP) means, with the

upload data being the unique embedded, media ticket smart card access code means with 1st example unique access code means being passphrases/passcodes, and 2nd example unique access code means being passwords with vowels automatically replaced by pseudo-random noise, and a 3rd example access code means being unique bio-identification such as a digital fingerprint transmitted over wiretapable ("red") computer buses from the media ticket smart card to the cryptographic digital signal processor (C-DSP) means,

decrypting using decryption from the relevant pass-thru encrypting means from said media ticket smart card upload to said cryptographic digital signal processor (C-DSP) means with 1st example pass-thru decryption means by the cryptographic digital signal processor (C-DSP) means using the system family key, fak-F, and 2nd example pass-thru decryption means being a family key encrypted index to a pre-embedded, common, vendor key look-up table to give efficient table look-up of the pre-stored, matching unique vendor public key, all sub-steps performed by the cryptographic media player of the customer's media ticket smart card access code in 1st example access code means being passphrases/passcodes, 2nd example access code means being passwords with automatically mixed in pseudorandom noise called salt, and 2nd example access code means being bio-identification such as digital fingerprints with added incremented sequence number used to prevent recorded replay attacks,

verifying against recorded replay attacks by provided, said new art, cryptographic digital signal processor [C-DSP] structural means inside of the provided, said cryptographic media player [C-MP] structural means,, by checking for an incremented sequence number, which can only be incremented by the media distribution vendor or else any provided, said new art, cryptographic media player [C-MP] structural means,, over the previous recorded sequence number in local provided, said prior art, cryptographic memory [TNV-EEPROM], which is the retrieved previous access of the same, provided, said media ticket smart card, sequence numbered play code and sequence numbered play count received from the media ticket smart card, and then the incrementing of the sequence number by the cryptographic media player,

doing the reverse step of encrypting using pass-thru encryption return means to download digital data from the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, to provided, said media ticket smart card, with the digital data being the smart card access code with incremented sequence number,

authenticating by customer triangle authentication of the following points:

point 1 of customer, party a, smart card access code comprising of a first example access code means of a

passphrase-passcode, a second example access code means of a password with automatic random noise (called 'salt') added to the entry, and a third example access code means of a bio-identification such as a digital fingerprint, to

point 2 of media ticket smart card a, to

point 3 of authorized cryptographic media player,

whereby this process claim has accomplished a relatively low rate of hacker breaching and high digital security, process called customer triangle authentication, which through this process has electronically and uniquely with very high probability of security authentication of involved parties, linked by use of this provided, said new art, cryptographic media player [C-MP] structural means, executed process claim, the 3-sided geometric triangle of: point 1: the relatively very high probability presence, of the warm blooded, registered unique customer ID, point 2: the registered said custom cipher-text digital media, and point 3: the said system party s only authorized digital media players.

83. (NEW) The invention and processes of claim 66 whereby the process of steps to do transferring of the cryptographic keys from provided said media ticket smart card to provided, said new art, cryptographic media players [C-MP's] structural means, with its provided said, new art, cryptographic digital signal processor [C-DSP] structural means, by said encrypting using pass-thru encryption means for the upload of digital data from said media ticket smart card to provided said, new art, cryptographic digital signal processor [C-DSP] structural means, over wiretapable or open computer buses ['red buses'] which is the process done by the provided, cryptographic media player to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n which are pass-thru encrypted by the several pass-thru encryption means involving several processes and components for transfer over wiretapable computer buses ['red buses'] to the player's own said cryptographic memory [TNV-EEPROM] for access by its said cryptographic digital signal processor [C-DSP] structural means, with said 1st example pass-thru encryption means being the common family key encryption vulnerable to a single point of attack, a said 2nd example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said 3rd example means of pass-thru encryption being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key

encrypted, common table index or vendor ID number for efficient active table entry access, comprising of the sub-steps of:

requesting by provided, said new art, cryptographic digital signal processor [C-DSP] structural means, sending a request digital code to the media ticket smart card A to request return of a pre-determined digital message code or else cryptographic key data which is pass-thru encrypted by various means with first pass-thru encryption means being the common system family key [fak-F] which is a known weak point in the system if the shared family key is breached, second pass-thru encryption means being a specific vendor's private key [prk-Vn] encryption done by the media ticket smart card which is pre-programmed with a common, pre-embedded, vendor key look-up table using a family key encrypted index for efficiency in processing on the other end, thus it is preceded by said family key [fak] encrypted index to the pre-embedded, common, vendor key look-up table for fast table look-up of the matching vendor public key also pre-programmed in provided, said cryptographic digital signal processor [C-DSP] structural means, on the other end,

transferring by the media ticket smart card n to provided, said cryptographic digital signal processor [C-DSP] structural means, of said return pre-determined digital message code or else said requested cryptographic keys comprising of customer private key [prk-n], encrypted play codes [session keys or one-time secret keys] with header, encrypted play counts [paid for numbers of plays, -1 for infinite plays, or counts of free trial plays] with

header all with sequence numbers to prevent recorded replay attacks,

decrypting by provided, said cryptographic digital signal processor [C-DSP] structural means, of the returned pass-thru encrypted cryptographic keys from the media ticket smart card using its pass-thru encryption means with first pass-thru encryption means being the trusted family key (which is vulnerable to leakage) to decrypt the pass-thru encrypted cryptographic keys, second pass-thru encryption means being the unique vendor public key which is pre-programmed using an embedded, common, vendor key look-up table for all vendors into said cryptographic digital signal processor (C-DSP) means and is preceded by a family key (fak) encrypted index to said vendor key look-up table for efficient table look-up without search time,

verifying by provided, said cryptographic digital signal processor [C-DSP] structural means, of incremented sequence numbers used to prevent a recorded replay attack (instead of requiring synchronized system clocks and time-stamped data) in the cryptographic keys returned from the media ticket smart card in order to prevent recorded replay attacks which is the sub-step done by provided, said cryptographic digital signal processor [C-DSP] structural means, using its locally cryptographically stored trusted family key [fak-F], customer private key (prk-n) retrieved from the customer's media ticket smart card, vendor public key [puk-Vn], and vendor secret key [sek-Vn] retrieved from local cryptographic memory [TNV-EEPROM], to pass-thru decrypt the

sequence numbers and check for an incremented value over the previous values stored in local cryptographic memory (only an authorized cryptographic media player can increment the sequence number before storage as only an authorized media distribution vendor or any cryptographic media player has the cryptographic keys to alter a sequence number),

storing by provided, said cryptographic digital signal processor [C-DSP] structural means, in its own local cryptographic memory [TNV-EEPROM] of the media ticket smart card's verified and decrypted cryptographic keys composed of the customer's private key, PrK-n, decrypted play count with header, decrypted play code with header in its own local tamper resistant non-volatile memory [TNV-EEPROM], this process must be followed by,

incrementing of sequence number function done by the provided, said cryptographic digital signal processor [C-DSP] structural means, and an opposite direction transferring function by the provided, said cryptographic digital signal processor [C-DSP] structural means, to the media ticket smart card of the updated cryptographic keys with incremented sequence number in order to avoid their rejected use in the future,

n-way committing of the previous sub-step to ensure sub-step completion in the event of unexpected circumstances such as but not limited to: power outages, pre-maturely customer withdrawn smart cards, and hardware failures, furthermore, failure to minimum 2-way

commit the above sub-step will completely void the entire operational step before anything is given the system go-ahead,

whereby this process claim has achieved, a relative high probability for commercial strong cryptography standards, and also commercial hardware standards, while still maintaining a commercially acceptable level of customer use, commercial convenience, and very low-cost standards of commercial use, furthermore, this process claim has insured a very low probability of hacker access, and a very low probability of falsified or non-authorized system hardware in use.

84. (NEW) The invention and processes of claim 66 whereby the process of steps to do transferring of the cryptographic keys away from provided, said new art, cryptographic media player [C-MP] structural means, and its internal provided, said new art, cryptographic digital signal processor [C-DSP] structural means, to provided, said prior art, media ticket smart card, by said encrypting using pass-thru return means, for the download of digital data from the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, to the provided, said prior art, media ticket smart card, over wiretapable or open computer buses ['red buses'] which is the process done by the provided, said new art, cryptographic media player [C-MP] structural means, which are pass-thru encrypted by the several pass-thru encryption means for transmit using it's provided, said cryptographic digital signal processor [C-DSP] structural means, the encrypted play codes with header and encrypted play counts with header both with provided, said cryptographic digital signal processor [C-DSP] structural means, incremented sequence counts [to avoid recorded replay attacks without the use of synchronized digital clocks] to the provided said, media ticket smart card A, transferred over wiretapable computer buses, with said 1st example pass-thru encryption means being the common family key encryption vulnerable to a single point of attack, a said 2nd example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said 3rd example means of pass-thru encryption

being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access, comprising of the sub-steps of:

transferring by pass-thru encrypting means by the provided, said crypto graphical digital signal processor [C-DSP] structural means, to the provided, said media ticket smart card, with 1st example pass-thru encryption means being common family key encryption which is known as being vulnerable to system breaching, and 2nd example pass-thru encryption means using a unique vendor public key for encryption which is first identified by a family key encrypted index to a pre-embedded, common, vendor public key and private key look-up table, which furthermore, enables the unique and matching vendor private key table look-up on the receiving end, furthermore, pass-thru encryption means is used in the process of transferring cryptographic keys comprising of customer private key [prk-n], encrypted play codes with header, encrypted play counts with header, all with already incremented customer [family key] sequence numbers from itself to the media ticket smart card,

decrypting of pass-thru encrypted means for cryptographic key transfer by the media ticket smart card which is the process done in first example pass-thru decryption means by using its trusted family key, and second example pass-thru decryption means being the use of said unique vendor public key which is identified for efficiency by said family key encrypted index, to decrypt the pass-

thru encrypted cryptographic keys from the provided, said cryptographic digital signal processor [C-DSP] structural means,

verifying of incremented customer [family key] sequence numbers to prevent recorded replay attacks which is the sub-step done by the provided, said cryptographic micro-processor [C-uP] embedded inside of the provided, said media ticket smart card using its local provided, said cryptographically stored inside of cryptographic memory [TNV-EEPROM], enabling the structural means of pass-thru encryption means first pass-thru encryption example means of a trusted family key [fak-F], and second example pass-thru encryption means example of a single vulnerable to breaching, pre-stored, family key [fak-F], indexed set of all vendor keys to efficiently retrieve the unique matching vendor public key to the unique vendor private key used, with pass-thru decryption means used to pass-thru decrypt the play code with header [and sequence numbers]:

removing the message authentication code [mac code] of the public vendor identification number,

removing the session identification number,

removing the customer [pass-thru encryption use] sequence number,

leaving the last to first by initial vendor media distribution center operation, customer public key encrypted, vendor secret key

encrypted, vendor digitally signed both of play code and vendor sequence number,

checking by the media ticket smart card for an incremented

customer (pass-thru encryption use) sequence number to prevent a recorded replay attack,

storing of cryptographic keys which is the sub-step done by the provided, said cryptographic micro-processor [C-uP] embedded inside of the provided said, media ticket smart card, storing the pass-thru decrypted keys including the customer's private key [PrK-n], decrypted updated play count with header, decrypted play code with header all with updated sequence numbers into its own local provided, said tamper resistant non-volatile memory [TNV-EEPROM],

returning of error status from the provided, said, media ticket smart card's, internal provided, said cryptographic micro-processor [C-uP] back to the provided, said cryptographic digital signal processor [C-DSP] structural means, which are the sub-steps of the provided, said media ticket smart card, composing a pre-determined digital error warning code or normal status warning with the looped back sequence number which is pass-thru encrypted and returned to the provided, said cryptographic digital signal processor [C-DSP] structural means,

whereby this process claim has achieved a relative, anti-hacker process, implemented in a relative manner commensurate for commercial cryptography security, especially guarding against illegal wiretapping illegal breaches, furthermore, guarding against recorded replay hacker attack breaches.

85. (NEW) The invention and processes of claim 66 whereby the process of steps to do authenticating using media triangle authentication which is the process of matching unique digital media with matching unique play codes by the method of media triangle authentication, which is the process done by provided, said cryptographic media player's [C-MP's] embedded, provided, said cryptographic digital signal processor [C-DSP] structural means, doing digital media triangle authentication using sample reads of test data with successful decryption, accomplished through the sub-steps of:

initializing before playing by the customer, party a, of the provided, said cryptographic digital signal processor [C-DSP] structural means through the process ~~of claim~~ 79,

reading by the provided, said cryptographic digital signal processor [C-DSP] structural means, of the custom encrypted digital media to obtain the public vendor identification number and session identification number of the particular media indexed by the provided, said cryptographic digital signal processor [C-DSP] structural means identification number,

{

public vendor identification number [MAC[VIN]],

session identification number,

play code encrypted digital media,

]

encrypting by the provided, said cryptographic digital signal processor [C-DSP] structural means, by using pass-thru encryption means with the 1st example pass-thru encryption means [vulnerable to system breaching] being the system family key [fak-F], family key encryption, and the 2nd example pass-thru encryption means being the unique vendor private key encryption with the additional family key encryption of an index used for efficiency to a pre-embedded, common, look-up table of vendor public and private keys, furthermore, with all pass-thru encryption means, the media's public vendor identification number and session identification number are used with an incremented sequence number to prevent recorded replay attacks,

transferring by the provided, said cryptographic digital signal processor [C-DSP] structural means, to the media ticket smart card inserted into a built-in media ticket smart card reader of the media's pass-thru encrypted public vendor identification number and session identification number with an incremented sequence number,

decrypting by the provided, said media ticket smart card using pass-thru decryption means with 1st example pass-thru decryption means using said system family key [fak-F], and 2nd example pass-thru decryption means using said unique vendor public key which is efficiently table look-up processed on the receiving end using the family key encrypted index to the common, pre-stored, vendor key table, furthermore, the pass-thru encryption means are used on the

media's public vendor identification number and session identification number with an incremented sequence number to prevent recorded replay attacks,

verifying by the media ticket smart card against recorded replay attacks in the decrypted data by checking for an incremented sequence number over the provided, said internal cryptographic memory [TNV-EEPROM] of the stored previous recorded sequence number access, indexed with the same provided, said cryptographic digital signal processor [C-DSP] structural means, identification number,

retrieving by the provided, said media ticket smart card n, from its internal provided, said cryptographic memory [TNV-EEPROM] in its internal public vendor identification number table, the session identification number of the matching encrypted play codes with header and encrypted play counts with header plus its own customer private key, prk-a,

notifying by the media ticket smart card back to the provided, said cryptographic digital signal processor [C-DSP] structural means of a custom encrypted digital media to media ticket smart card pre-determined digital code, only for a mismatch error status going back, if the public vendor identification number and session identification number search produces no matches in provided, said local cryptographic memory [TNV-EEPROM],

decrypting by the provided, said cryptographic digital signal processor [C-DSP] structural means always in the exact reverse

order of encryption in order to mathematically undo encryption operations in the proper sequential order, using pass-thru decryption means with 1st example pass-thru encryption means being the common system family key [fak-r], and 2nd example pass-thru encryption means being the unique vendor public key with a family key encrypted index to a pre-embedded, common look-up table of vendor public and private keys for efficient table look-up, and decryption using the vendor private key [prk-Vn], and vendor secret key [sek-Vn], out of the set of all vendor public keys and vendor secret keys retrieved from provided, said local cryptographic memory [TNV-EEPROM], by the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, used upon the customer's encrypted play code with header, play count with header, and private key [prk-a], with sequence number to prevent recorded replay attacks,

verifying against recorded replay attacks by the provided, said cryptographic digital signal processor [C-DSP] structural means by checking for an incremented sequence number over the previous recorded sequence number access of the same provided, said media ticket smart card, held in internal provided, said prior art, cryptographic memory [TNV-EEPROM],

incrementing by the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, of the customer [family key] sequence number received from the provided, said media ticket smart card,

encrypting by the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, using pass-thru encryption means with 1st example pass-thru encryption means being the system family key [fak-r], and 2nd example pass-thru encryption means being the unique vendor private key with a family key encrypted index to a table of vendor keys for efficiency, of the media ticket smart card's retrieved encrypted private key [prk-a], encrypted play codes with header, and encrypted play counts with header, all with an incremented sequence number to prevent recorded replay attacks,

transferring using pass-thru encrypting means by the provided, said cryptographic digital signal processor [C-DSP] structural means, to the media ticket smart card of the updated cryptographic keys comprising of customer party a's private key [prk-a], encrypted play codes [session keys or one-time secret keys] with header and encrypted play counts [paid for numbers of plays, exampled by constant -1 binary encoded as meaning infinite plays, or counts of free trial plays] with header and all with sequence numbers by the process of claim 77,

authenticating of the media triangle authentication by the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, which is the sub-step done by the provided, said, new art, cryptographic digital signal processor [C-DSP] structural means, contained inside of the provided, said new art, cryptographic media player [C-MP] structural means,, decrypting a sample known test pattern of the digital media by using the

decrypted play code [session key or one-time secret key] stored inside of internal provided said, cryptographic memory [TNV-EEPROM] inside of the provided, said cryptographic digital signal processor [C-DSP] structural means also with using the vendor's public key [puk-Vn], and vendor's secret key [sek-Vn], in order to undo the pass-thru encrypting means processes of claim 77, using the following data structures:

unique vendor and customer play count with media header [and sequence number] is:

[

public vendor identification number [MAC[VIN]],

session identification number,

customer A public key encrypted

[vendor secret key encrypted

[vendor private key digitally signed[

play count, sequence number}]]

customer [pass-thru encryption use] sequence number,

] - tcmp-16a,

vendor pass-thru encrypted play count with media header [and sequence numbers] is:

family key [temp-16a] = temp-16b,

unique vendor and customer play code with media header (and sequence numbers) is:

[

public vendor identification number [MAC[VIN]],

session identification number,

customer A public key encrypted

[vendor secret key encrypted

[vendor private key digitally signed

[play code, sequence number]]

customer (pass-thru encryption use) sequence number,

]

] = temp-16c,

vendor family key encrypted or pass-thru encrypted means of the play code with media header and sequence number is:

family key [temp-16c] = temp-16d,

and then using the decrypted play code also known as a session key or one-time secret key for decrypting the custom encrypted digital media which known sample data area will only decrypt properly to a known test pattern with the proper untampered with play code,

authenticating with media triangle authentication by the provided, said cryptographic digital signal processor [C-DSP] structural means of the following points:

point 1 of custom, encrypted digital media a, to

point 2 of media ticket smart card a, to

point 3 of authorized cryptographic media player,

whereby this process claim has achieved, a relative guarantee of unique authenticity of the 3 geometric points of: point 1 of custom, encrypted digital media a, to point 2 of media ticket smart card a, to point 3 of authorized cryptographic media player, furthermore, guarding and warning the customer against the frequently occurring common problem, of inserting the wrong match of said custom digital media and said smart card.

86. (NEW) The invention and processes ~~of claim~~ 66 whereby the process of steps to do cryptographing using hybrid key cryptography which is the process done by provided, said cryptographic media player [C-MP] structural means,, with its provided, said embedded provided, said cryptographic digital signal processor [C-DSP] structural means, with further, provided said cryptographic memory [TNV-EEPROM], using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys [ssk-n], used for only one session, which said session keys are sent to a remote party, who decrypts them for storage in his own provided, said tamper resistant, non-volatile memory [TNV-EEPROM] embedded on his black, cryptographic computing unit in the example of the prior art, provided, said cryptographic digital signal processor [C-DSP] structural means, which said session keys may be later stored in provided, said tamper resistant non-volatile memory [TNV-EEPROM] embedded in a provided, said media ticket smart card, where they are referred to as play codes with paid for and authorized play counts, accomplished through the sub-steps of:

authenticating of play code digitally signed by the authorized media distribution vendor's private key to the provided, said cryptographic digital signal processor [C-DSP] structural means, which is the sub-step done by the provided, said cryptographic digital signal processor [C-DSP] structural means, which holds the

complete public key set of all authorized media distribution vendors retrieving the play code from the media ticket smart card A and using the correct vendor public key to decrypt the session key which was digitally signed by the vendor private key to reveal the decrypted session key ready for use on the custom encrypted digital media,

decrypting of the custom encrypted digital media which is the sub-step done by the provided, said cryptographic digital signal processor [C-DSP] structural means, using the decrypted session key or 1-time use only secret key, for secret key decrypting means involving one or more processes and components, with the 1st example secret key decrypting means being slower, software algorithm secret key cryptographing, and the 2nd example secret key cryptographing means being fast, hardware secret key cryptographing, with both example decrypting means loading the session key or one-time use only secret key into the cryptographic digital signal processor's [C-DSP's] structural means, hardware secret key unit which can decrypt the custom encrypted digital media,

whereby this process claim has achieved, by use of provided said, prior art, hybrid key cryptography algorithms, a very low probability of hacker intercept, also relatively very high speed encryption and decryption, whereby the provided, said prior art, secret key algorithm encryption speed, is a relative high execution speed, being from 10

times in hardware, up to 100 times in software, faster than comparable, the public key or asymmetric encryption and public key decryption, furthermore, obtaining the advantage of provided, said prior art, secret key cryptography algorithm of relatively strong, authentication of remote parties, furthermore, execution in provided, said new art, cryptographic media players [C-MP] structural means, has greatly improved the integrity and digital security of execution firmware and cryptographic keys in transit, and also cryptographic storage only in provided, said tamper resistant non-volatile, electrically erasable programmable read-only memory [TNV-EEPROM].

87. (NEW) The invention and processes of claim 86 whereby the process of steps to do public key cryptographing which is the process done by provided, said new art, cryptographic media player [C-MP] structural means, and its provided, said new art, cryptographic digital signal processor [C-DSP] structural means, and internal provided, said prior art, cryptographic memory [TNV-EEPROM], accomplished through the sub-steps of:

authenticating of play code digitally signed by the use of the unique and appropriate authorized media distribution vendor's private key which is pre-stored before factory release of the hardware chip in a common look-up table in the provided, said cryptographic digital signal processor [C-DSP] structural means, which is the sub-step done by the provided, said cryptographic digital signal processor [C-DSP] structural means, which holds the complete, pre-embedded, common look-up table, vendor indexed, private key and public key set of all authorized media distribution vendors, which provided, said cryptographic digital signal processor [C-DSP] structural means, uses pass-thru encrypting process 80 and pass-thru encrypting return process 81, to first retrieve the play code from the provided, said media ticket smart card a, for customer party a, and pass-thru decrypt the play code, and then uses the correct vendor public key from the pre-embedded, common look-up table, vendor indexed, vendor private key and public key set of all authorized media distribution vendors, to digital

signature verify the presently non-cipher text or presently signatured text of the unique, session key, which was already digitally signed by the use of the unique, media distribution vendor private key at downloading to customer A of process 75 or also called media distribution time, to reveal the decrypted session key ready for use on the custom-encrypted digital media,

whereby this process claim has achieved, a very low probability of hacker intercept, provided, said prior art of public key cryptography algorithm used in conjunction with a provided, said new art, cryptographic media player [C-MP] structural means,, to provide relatively strong remote authenticity of remote parties.

88. (NEW) The invention or processes of claim 86 whereby the process of steps to do secret key cryptographing which is the process done by provided, said cryptographic media player [C-MP] structural means, with its embedded, provided, said cryptographic digital signal processor [C-DSP] structural means, through certain applicable sub-steps selected from the group comprising of:

decrypting of the custom encrypted digital media using software algorithm, slower, double secret key cryptographing, which is the sub-step done by the provided, said cryptographic digital signal processor [C-DSP] structural means, using the decrypted session key (one-time secret key) from the matching unique play code for slower, software algorithm implemented by firmware computer program secret key cryptography, without use of a silicon compiler designed, dedicated fast hardware secret key unit, by loading said decrypted session key or one-time secret key into the cryptographic digital signal processor's (C-DSP) means which can software decrypt the custom encrypted digital media, furthermore, with exactly analogous firmware secret key decryption using the unique vendor secret key, and,

decrypting of the custom encrypted digital media which is actually double secret key encrypted, first with the unique originating vendor secret key and secondly with the unique customer session key or one-time use only secret key, using a silicon

compiler designed duo-unit specifically doing, fast, hardware double secret key cryptographing, which is the sub-step done by the cryptographic digital signal processor (C-DSP) means using the unique customer decrypted session key (one-time secret key) from the unique relevant play code for fast, hardware secret key cryptographing by loading said decrypted session key or one-time secret key into the cryptographic digital signal processor's (C-DSP) means, silicon compiler designed, prior art, specific hardware secret key unit which can fast hardware decrypt the custom encrypted digital media, followed in an exactly similar manner by the hardware loading of the unique vendor secret key,

whereby this process claim has achieved implementation of a very low probability of hacker intercept, provided, said prior art, secret key cryptography, used with provided, said new art, cryptographic media player [C-MP] structural means,, which has provided relatively, very fast execution encryptions and decryptions of customer cipher text digital media.

89. (NEW) The invention or process of claim 88 whereby the process of secret key cryptographing uses standardized, algorithm means involving several processes and components of a first algorithm means being older and field and time proven but of growing obsolescence, bit oriented (approximately ten to one-hundred times faster when executed in a dedicated bit-manipulative digital hardware silicon compiler designed library component unit), US Patented (expired), IBM Data Encryption Standard (DES), which comes in several modes and secret key strengths measured in key bit-length, and a second algorithm means being newer, fully unproven algorithm in both field and time trials, a byte (8-bit) oriented, Advanced Encryption Standard (AES) cipher which was designed for faster, software algorithm implementation and scalability of the bit-length of increasing key strength with time to deter scalable computing attacks on fixed length secret key length, and third example secret key algorithm means being newer, field and time proven, fixed secret key length, IDEA (R), under European patent,

whereby this process claim has achieved, various design goals of security, efficiency in execution time and bit-length of keys, and also has enabled, future automatic compensation for by the algorithm, of future anticipated to counter future hacker threats, secret key bit-length expansion.

90. (NEW) The invention and processes of claim 66 whereby the process of steps to do accounting by the provided, said new art, cryptographic media player [C-MP] structural means, with its provided, embedded said cryptographic digital signal processor [C-DSP] structural means, which is the process done by the provided, said new art, cryptographic media player [C-MP] structural means, using hybrid key cryptography digital media playing of one-way transfer of custom session key encrypted digital media owned by party n, in a controlled access manner mostly for financial accounting purposes which uses the play codes [session key or one-time secret key] and play counts [paid for number of plays or count of free trial plays] contained in media ticket smart cards, accomplished through the sub-steps of:

authenticating step done in high security applications which sub-process step is simply skipped as being unnecessary in low security applications for citizen/customer time and effort consideration, of customer triangle authenticating using the process of claim 85 of:

point 1 of customer a, to

point 2 of media ticket smart card a, to

point 3 of cryptographic media player,

authenticating of the media triangle authenticating by the process of claim 81 comprising of:

point 1 of one-way transfer of custom session key encrypted digital media, to

point 2 of media ticket smart card A with appropriate play codes and play counts, to

point 3 of cryptographic media player,

notifying of the customer of any errors in the above two sub-steps, transferring by the media ticket smart card to the cryptographic digital signal processor (C-DSP) means of the pass-thru encrypting means of cryptographic keys comprising of customer private key (PrK-n), play count with header, and play code with header all with sequence numbers using the process ~~of claim~~ 40,

verifying of decrypted play count greater than one which is the sub-step done by a cryptographic digital signal processor (C-DSP) means inside of a cryptographic media player checking the obtained decrypted play count for a greater than one number indicating authorized and paid for plays remaining while a -1 value for a count can be a means of indicating an infinite number of plays,

decrementing of play count which is the sub-step done by the cryptographic digital signal processor (C-DSP) means of decrementing of the play count,

incrementing of customer (pass-thru encryption use) sequence number by the cryptographic digital signal processor (C-DSP) means to prevent recorded replay attacks,

transferring by the cryptographic digital signal processor (C-DSP) means to the media ticket smart card of the pass-thru encrypting return means of process 78 of the updated for sequence number cryptographic keys comprising of customer private key (PrK-n), and the updated for sequence number and accounting decrements both the play count with header, and the play code with header all with incremented sequence numbers,

whereby this process step has implemented through said commercial said parties vn, and also private digital media origin parties, financial cost controls and count controlled plays through said play counts and said play codes of said custom encrypted digital media or custom cipher text digital media, while at the same time not impacting non involved digital media.

91. (NEW) The invention and processes of claim 66 whereby the process of steps to do playing by provided, said new art, cryptographic media player [C-MP] structural means, with its provided, said new art, cryptographic digital signal processor [C-DSP] structural means, which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or one-time secret keys) and play counts (now contained within registers in provided, said cryptographic digital signal processor (C-DSP) means) and also the secret key decryption directly used upon the custom encrypted one-way transfer of custom session key encrypted digital media which is pre-unique vendor secret key encrypted, accomplished through the sub-steps of:

detecting of non-copyrighted commercial or home-made material through an absence of encryption through the use of media triangle authenticating of process 47 which will allow hardware decompression of standard form compressed digital media through prior art digital compression means such as Moving Picture Electronics Group X [MPEG X] for audio/video, Moving Picture Electronics Group Standards I Audio Layer 3 [MP3] for audio only, fast wavelet compression [Fraunhofer Institute of Germany's], artificial digital degradation, and digital to analog conversion [DAC] for analog output while skipping the following sub-steps,

cryptographing by the cryptographic digital signal processor [C-DSP] structural means, using hybrid key cryptography playing of the custom encrypted digital media using the process ~~of claim~~ 48 for the unique vendor secret key,

cryptographing by the cryptographic digital signal processor [C-DSP] structural means, using hybrid key cryptography playing of the custom encrypted digital media using the process 86 for the unique session key or one-time only use secret key obtained by said cryptographic digital signal processor (C-DSP) means from said unique play code or the pass-thru encrypted, unique decryption key (this is a very fast, double secret key decryption process which secures the decrypted ('plain text') digital masters to the exclusive knowledge of the unique media origination vendor who may or may not be the media distribution vendor) (remember that the unique encrypted ('cipher-text') digital media is completely useless without the corresponding matching said play code or decryption keys, and said non-zeroed remaining play, play count, or accounting charges),

accounting by the cryptographic digital signal processor [C-DSP] structural means, of the custom encrypted digital media using the process of claim 90,

whereby the present process claim has played said custom digital media or said custom encrypted digital media, which was said

commercial party vn, and also private parties of digital media creation, turned into a controlled system process only as enabled by this process.

92. (NEW) The invention and processes of claim 66 whereby the process of steps to do escrowing retrieval of lost, stolen, or disputed legal ownership media ticket smart cards, as well as custom cipher text digital media distribution material, which is the process done by the given customer, party a, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of 'de facto,' and then internationally standardized cryptography sanctioned by industry trade groups such as the Recording Industry Association of America's [RIAA's] Secure Digital Music Initiative [SDMI], the National Association of Broadcaster's [NAB's] Secure Digital Broadcast Group [SDBG], accomplished through the sub-steps of:

reporting of lost, stolen, or disputed legal ownership media ticket smart cards by the customer, party a, to the central public key distribution authority, party d,

canceling of the existing card by the public key distribution authority, party d, in its customer database,

retrieving by the central public key distribution authority, party d, from the central public key escrow authorities, parties en, of the old customer public key pair,

issuing of a new card by the public key distribution authority, party d, with a new customer public key pair,

retrieving by the central public key distribution authority, party d, from all media distribution vendors, parties vn, of existing partially encrypted customer's, party a's, play codes and play counts stored in computer database (which will not have the latest play count of the lost card which does not matter for infinite plays or free trial plays and financial compensation can be made for finite play counts) from all download sessions which can be restored with customer's, party a's, new public keys done by the process of:

```
d-prk-a-old(
   remove mac(vin),
   remove session identification number,
   remove customer (pass-thru encryption use) sequence number,
   (d-fak-F
            (pass-thru encrypted play code with
                  header (and sequence numbers)
            ),
   )) - tcmp-23a,
d-prk-a-old (
   remove mac(vin),
```

remove session identification number,

remove customer (pass-thru encryption use) sequence number,

(d-fak-F

(pass-thru encrypted play count (with sequence numbers)

),

)) = temp-23b,

imprinting the customer's, party a's, old play codes and play counts into the new media ticket smart card,

d-fak-F(

mac(vin),

session identification number,

d-puk-a-new(temp-23a),

customer (pass-thru encryption use) sequence number + 1) =

(new encrypted play code with header (and sequence numbers),

d-fak-F(

mac(vin),

session identification number,

d-puk-a-new(temp-23b),

customer (pass-thru encryption use) sequence

number + 1) =

(new encrypted play count with header (and sequence

numbers),

delivering of the reconstructed, new media ticket smart card to the customer parties a, b, c, i to z, which should work with existing custom encrypted media and it will still work with the lost, stolen, or legally disputed old media ticket smart card,

whereby the present process claim has implemented through the minimal, said 3-layer federated system of cryptographic this process claim's layers: while for broader process claims purposes, counting as only 1 a combined middle 2 of 4 said relevant patent drawing layers, combined for broader claims purposes into 1 layer, or combining the relevant patent drawing's middle 2 layers into 1 layer for broader

claims purposes, as 1 layer: a combined middle layer for both commercial hardware vendors and commercial digital media vendors, furthermore, implementing by this process an assumed design rule of having no inherent hardware and firmware secrecy, no hidden wiretapping points, and also no double key spaces, furthermore, the minimal said 3-layer federated system of cryptographic layers of this process claim's layers: the bottom-most relevant patent drawing layer, being the highest cryptographic system architecture layer of said system keys under said system party s, in which this system party s's administration through said whole key generation party g, who has been given 100% whole key knowledge, but, 0% knowledge of customer identifications, which are known only to said whole key distribution party d, furthermore, party s also having a minimum of 2 units of said spit key distribution parties sn, each parties sn having securely received secure, split key relational databases, furthermore, the parties sn only having allowed through this process, top secret, unique customer secret index based whole key re-generation, upon customer request for a lost, stolen, or disputed legal ownership said smart card.

93. (NEW) The invention and processes of claim 92 whereby the process of steps to do legal re-assigning of play code and play count ownership from media ticket smart A of owner A to media ticket smart card B of owner B which is legally called "first use" involving US Copyrighted digital media which is accomplished through the sub-steps of:

inserting of media ticket smart card A into the cryptographic digital signal processor (C-DSP) means inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using the already defined process 81 of authenticating by customer triangle authentication,

transferring of all customer A play codes and play counts from the media ticket smart card A into the cryptographic digital signal processor (C-DSP) means including the customer A's private key and public key,

decrypting of customer A's play code and play count,

updating of vendor sequence number and customer (pass thru encryption use) sequence number,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor (C-DSP) means to media

ticket smart card and back again before finalizing transaction computer operations,

permanently erasing in media ticket smart card A any removed play codes and play counts owned by customer A,

removing of the customer A's media ticket smart card from the cryptographic media player,

inserting of media ticket smart card B into the cryptographic digital signal processor (C-DSP) means inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication,

transferring of all customer B play codes and play counts from the media ticket smart card B into the cryptographic digital signal processor (C-DSP) means including the customer B's private key and public key,

decrypting of customer B's play code and play count,

creating a super-set list of play codes and play counts and re-encrypting them for customer B,

updating of vendor sequence number and customer (pass-thru encryption use) sequence number,

transferring the super-set list of play codes and play counts back to media ticket smart card b for cryptographic storage,

committing a minimum of 2-way operations of several cyclic loops from cryptographic digital signal processor (C-DSP) means to media ticket smart card and back again before finalizing transaction computer operations,

permanently erasing all play codes and play counts of either party a or party b, from the cryptographic media player,

removing of the customer party b's media ticket smart card from the cryptographic media player,

whereby this process claim has implemented, the US copyright law's legal doctrine of 'first use,' by having used in the proximate prescribed manner, provided, said media ticket smart cards, and also by having used in the proximate prescribed manner, provided, said cryptographic media players [C-MP's].

94. The invention and processes of claim 92 whereby the process of steps to do legal archiving of custom encrypted digital media and also play code and play count ownership from media ticket smart A of owner A to back-up copies known as legal "fair use" under US Copyright law for means of archival storage in case of fire, theft, vandalism, storm, flooding, for a convenient home and car copy for marketing applications of the "fair use" legal doctrine, which is accomplished by the sub-steps of:

copying of "cipher text (encrypted data)" digital media in digital to digital copying mode an unlimited number of times using a personal computer [PC] or other digital to digital copying device to create flawless digital archival copies which are usable only with media ticket smart card A primary card or media ticket smart card A back-up card,

updating of primary card to back-up card operations to allow both to be used for archival copy decryptions,

inserting of media ticket smart card A primary card into the cryptographic digital signal processor (C-DSP) means inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication by the process of claim 81,

transferring of all customer A primary card play codes and play counts from the media ticket smart card A into the cryptographic digital signal processor including the customer A's private key and public key,

decrypting of customer A's primary card play code and play count,

updating of vendor sequence number and customer (pass-thru encryption use) sequence number,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor (C-DSP) means to media ticket smart card A primary card's tamper resistant non-volatile memory (TNV-EEPROM) and back again before finalizing transaction computer operations,

permanently erasing in media ticket smart card A primary card's tamper resistant non-volatile memory (TNV-EEPROM) any removed play codes and play counts owned by customer A,

removing of the customer A's media ticket smart card primary card from the cryptographic media player,

inserting of media ticket smart card A back-up card

into the cryptographic digital signal processor (C-DSP) means inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication by the process of claim 81,

transferring by pass-thru encrypting means of all customer A back-up card play codes and play counts from the media ticket smart card A back-up card into the cryptographic digital signal processor (C-DSP) means including the customer A's private key and public key,

decrypting of customer A's play code and play count,

creating a super-set list of play codes and play counts and re-encrypting them for customer A,

updating of vendor sequence number and customer (pass-thru encryption use) sequence number,

transferring the super-set list of play codes and play counts back to media ticket smart card A back-up for cryptographic storage,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor (C-DSP) means to media ticket smart card A's tamper resistant non-volatile memory (TNV-EEPROM) back-up before finalizing transaction computer operations,

removing of the customer A's media ticket smart card back-up from the cryptographic media player,

inserting of media ticket smart card A primary card

again into the cryptographic digital signal processor (C-DSP) means inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication by the process of claim 81,

re-accessing in the cryptographic media player the already created super-set list of play codes and play counts and re-encrypting them for customer A,

updating vendor sequence number and customer (pass-thru encryption use) sequence number,

transferring the super-set list of play codes and play counts back to media ticket smart card A back-up for cryptographic storage,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor (C-DSP) means to media ticket smart card A back-up before finalizing transaction computer operations,

permanently erasing all play codes and play counts of either party a primary card or party a back-up card from the cryptographic media player,

removing of the customer a's media ticket smart card primary from the cryptographic media player,

whereby this process claim has implemented, the US copyright law's legal doctrine of 'fair use,' which has been implemented by this process claim, by use of provided, said media ticket smart cards and also provided, said cryptographic media players [C-MP's].

95. (NEW) A specific process for doing public key cryptography over an open systems architecture in a totally cryptographically secure manner meant for safeguarding multi-million dollar digital masters which open systems architecture includes existing prior art components to give a new art system of processes or a process patent of public key cryptography comprising of the process steps of:

providing of the component of prior art, a tamper-resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], with means for secure cryptographic key storage,

providing of the component of prior art, an electrically erasable programmable read-only memory (EEPROM),

providing of the component of prior art, a static random access memory [SRAM],

providing of the component of prior art, a dynamic random access memory [DRAM],

providing of the component of prior art, a low-cost, low-throughput, cryptographic micro-controller [C-u-CTLR], furthermore, which already contains provided, said prior art, a tamper-resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], with means for secure cryptographic key storage,

providing of the component of a prior art, smart card, with means for media ticket applications contained in provided, said prior art, cryptographic micro-controller's [C-u-CTLR's], furthermore, already containing of provided, said prior art, tamper resistant, non-volatile electrically erasable programmable read-only memory [TNV-EEPROM] which is used for secure cryptographic key storage,

providing of the component of a new art, smart card with bio-ID, with means for media ticket applications contained in provided, said prior art, cryptographic micro-controller's [C-u-CTLR's], furthermore, already containing of provided, said prior art, tamper resistant, non-volatile electrically erasable programmable read-only memory [TNV-EEPROM] which is used for secure cryptographic key storage, furthermore, a unique digital customer bio-ID is stored in the crypto-memory,

providing of the component of prior art, serial data computer communications interfaces such as a personal computer [PC] based, digital serial buses, with means to connect a personal computer [PC] to a digitized human fingerprint reader and for other computer peripheral purposes,

providing of the component of prior art, a smart card reader, with means for pass-thru encryption,

providing of the component of prior art, biological-identification [bio-ID] reader [bio-ID-reader] means which attach to personal computers [PC's], with means for reading of customer bio-ID,

digitization of such bio-ID, and pass-thru encryption meant to securely transfer such data to a hosting PC,

providing of the component of prior art, an internet protocol [IP], wide area network [IP WAN],

providing of prior art, a world wide web server [WWW] or web or graphics rich portion of the Internet web server computer,

providing of the component of prior art, a personal computer [PC], which is non-cryptographically secure,

providing of the component of prior art, a personal computer [PC] web client,

providing of the component of prior art, a personal computer [PC] peripherals,

providing of the component of prior art, a data entry devices of an on-board protected electronic device, toggle field with a prior art liquid crystal display [LCD] for entry of the unique customer passphrase with closely corresponding passcode entry,

providing of the component of prior art, a data entry device of computer keyboards, with means for customer entry of a unique customer password, and passphrase-passcode entry,

providing of the component of: provided said, prior art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-

text data sent to an attached provided, said prior art, digital serial bus, furthermore, 1st example means being digitized fingerprint bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of prior art, a banked-EEPROM card reader-writer, connected by a prior art, serial bus connected to a PC,

providing of the component of prior art, a personal computer's [PC's] peripheral data storage devices, with means for non-volatile or permanent computer memory whether removable or non-removable units,

providing of the component of prior art, a personal computer's [PC's] based peripheral data storage media units,

providing of the component of a provided said, new art, cryptographic digital signal processor [C-DSP], designed for low-cost, very fast digital processing of fixed-point number array or arrays of fixed radix numbers having limited necessary precision typically less than 32-bits arranged in matrix arrays (32-bit integers with an assumed radix point which cannot move with a default assumed decimal point which cannot move), also with means for containing said tamper resistant non-volatile read only memory [TNV-EEPROM],

providing of the component of prior art, a cryptographic digital signal processor [C-DSP], intended for very fast processing of large fixed-point arrays of fixed-point or fixed radix numbers, additionally containing a cryptographic hardware secret key algorithm sub-processor, as well as provided, said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], provided, said random access memory [RAM], analog to digital signal converters [ADC], moving picture electronics group standards X [MPEG X] hardware decompression only circuitry for digital audio/video, digital audio/video signal artificial degradation circuitry, digital to analog signal converters, and digital signal processing of digital audio/video signals circuitry,

providing of the component of new art, cryptographic digital signal processor [C-DSP], designed for low-cost, very fast, digital processing of fixed-point number arrays, furthermore, having additional silicon compiler designed components adding embedded provided, said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM] for secure cryptographic key storage, along with both tamper resistant to pin-probers, and cryptographically protected on-chip, firmware implemented new art, byte-oriented, secret key algorithm based secret key encryption and decryption for both stream oriented and block oriented encryption and decryption processes, with on-chip hardware and firmware library support for both secret key and public key algorithms such as an electronic true random number generator, an on-chip hardware floating point unit (FPU) for processing large blocks of secret key encrypted

and decrypted data using newer y. 2003 firmware based, byte oriented, secret key algorithms such as Advanced Encryption Standard (AES), an extremely large integer to an extremely large integer exponentiation unit using the binary square and multiply method commonly used in public key cryptography, with additional on-chip silicon compiler designed hardware support for digital decompression (read-only) algorithms, with additional on-chip silicon compiler support for digital compression algorithms, with additional on-chip silicon compiler support for forward error detection and correction coding (e.g. Reed-Solomon or RS coding) done in the encoding process sequential order of digitally compress, error correct, and encrypt, with decoding done in the exact opposite sequential process order, with a 1st example C-DSP means being discussed broadly in the present inventor's present patent's technical material which is not subject to this present over-all system's or methods patent application which uses such a device as a provided hardware component,

providing of the component of new art, programmable gate array logic [GAL] form of high density, application specific integrated circuit [ASIC] with embedded provided said, cryptographic digital signal processor [C-DSP] structural means, having functional means as mentioned in the paragraph just above,

providing of the component of new art, a cryptographic digital signal processor (C-DSP), furthermore, having cryptographic digital signal processor functionality,

providing of the component of a new art, a cryptographic micro-processor [C-uP], furthermore, having cryptographic digital signal processor functionality,

providing of the component of new art, a cryptographic computing based unit [C-CPU], furthermore, having cryptographic digital signal processor functionality,

providing of the component of new art, a cryptographic personal computer [C-PC], comprising of provided said, new art, cryptographic micro-processor unit [C-uP],

providing of the component of new art, a cryptographic personal computer [C-PC] having a subset functionality of a provided, said [C-DSP] structural means,

providing of the component of: provided said, new art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-text data sent to an attached provided, said prior art, digital serial bus, furthermore, attached to a provided, said new art, cryptographic PC [C-PC], furthermore, 1st example means being digitized fingerprint bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of new art, a highly secure, or cryptographic operating system (C-OS) for world wide web (WWW) server computers,

providing of the component of new art, a cryptographic media player (C-MP) structural means,

providing of the component of new art, a universal cryptographic set-top box, being a form of custom cryptographic digital media players (C-MP's) structural means,

providing of the component of new art, a cryptographic micro-mirror module (C-MMM) or commercial theater projection-theater sound units,

providing of the component of prior art, a modified secure operating system (secure-OS) for world wide web (WWW) server computers,

providing of the component of prior art, a world wide web (WWW) transmission control protocol-internet protocol (TCP-IP) command protocol stack program for Internet connectivity,

providing of the component of prior art, standard, a plurality of cryptographic mathematics algorithms,

providing of the component of prior art, a plurality of public key cryptography algorithms which create public keys and private keys,

providing of the component of prior art, a plurality of secret key cryptography algorithms which create secret keys and session keys (1-time secret keys) and also play counts or access counts or media decryption counts and play codes (session keys or 1-time secret keys),

providing of the component of prior art, a plurality of hybrid key cryptography algorithms which are combined public key and private key cryptography algorithms,

providing of the component of prior art, a plurality of private key and secret key splitting algorithms,

providing of the component of prior art, a plurality of private key and secret key escrow techniques,

providing of the component of prior art, a plurality of algorithms used to generate: cryptographic keys which are the collective public keys, private keys, secret keys, session keys (1-time use only secret keys), play counts, play codes, passphrases-passcodes,

providing of the component of prior art, a plurality of computer cryptography protocols,

providing of the component of prior art, a plurality of pass-thru encryption algorithms for transmitting secure data over wiretapable computer buses ['red buses'],

providing of the component of prior art, standardized form, a plurality of lossy compressed digital media algorithms,

providing of the component of prior art, a transmissions control protocol/internet protocol [TCP/IP] for Internet connectivity,

providing of the component of prior art, a secure internet protocol layer [secure IP layer] layer of Internet data encryption,

providing of the component of prior art, a secure sockets layer [SSL] layer of Internet data encryption,

providing of the component of prior art, a plurality of world wide web [WWW] server standard interchange file languages,

providing of the component of a plurality of world wide web [WWW] client standard interchange file languages,

generating of a set of common system keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

generating of a set of media distribution vendor cryptographic keys eventually used in cryptographic digital signal processors (C-DSP's) for eventual manufacturing into cryptographic media players which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

generating of a media ticket smart card cryptographic key set or unique customer cryptographic key set, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

distributing of provided, said cryptographic digital signal processors (C-DSP's), which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing of provided, said cryptographic digital signal processors [C-DSP's] structural means, given that party G has already pre-embedded an entire set of a unique per vendor, common cryptographic key table into each and every cryptographic digital signal processor [C-DSP] structural means, followed by party g's physical chip distribution to media distribution vendors, parties vn, for manufacturing into cryptographic media players, while parties vn have absolutely no access to whole cryptographic keys,

distributing of the provided, said media ticket smart cards which is the process done by the media ticket smart card system

authority's, party s's, dedicated public key distribution authority, party d, distributing provided, said media ticket smart cards to media distribution vendors, for selling to customers while having absolutely no access to whole cryptographic keys,

escrowing of the split cryptographic keys which is the process done by the central key generation authority, party g, safe-guarding the split cryptographic customer keys, and split cryptographic vendor keys in an entirely secure and confidential manner with legal first means for simple customer identification and lost key recovery, second means for disputed ownership court ordered recovery, and third means for court ordered only use by law enforcement,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with 3-layers, a bottom-most relevant patent drawing layer of highest cryptography and logic abstraction, composed of the media ticket smart card system authority, a 2 count of the middle-most relevant patent drawing, combined middle layer composed of authorized hardware vendor distribution companies, parties vn, also authorized media distribution companies, parties vn, and a top-most relevant patent drawing's user layer composed of customer parties: a, b, c, and i to z,

preparing of a unique play code and a unique play count which is the process done by the authorized digital media distribution company, party vn, preparing a unique play code or custom encrypted

session key or one-time use only secret key, a unique play count or custom encrypted paid for numbers of plays or counts of free trial plays, and custom encrypted digital media for downloading to each customer,

downloading to customer, party a, which is the process done by the authorized digital media distribution vendor, party vn, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a World Wide Web (WWW) server to multiple personal computer [PC] based World Wide Web (WWW) clients of encrypted play codes (one-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into media ticket smart cards attached to personal computer [PC] based media ticket smart card readers, and one-way transfer of custom session key or one-time secret key encrypted digital media which is pre-unique vendor secret key encrypted for deposit into physical digital media inserted into media drives attached to personal computers (PC's),

delivering by foot which is the process done by the customer, party a, of physically transferring both physical custom encrypted digital media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, personal computer to any person's cryptographic media player with a built-in media ticket smart card reader,

encrypting using pass-thru means involving several processes and components for transferring any type of digital data securely from the media ticket smart card up to the cryptographic digital signal processor (C-DSP) means with 1st example pass-thru encrypting means, being common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, 2nd example pass-thru encrypting means being a pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being a row, column table indexed by a vendor identification number, 3rd example pass-thru encrypting means being a pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being a row, column table indexed by a vendor identification number,

encrypting using pass-thru return means involving several processes and components for transferring any digital data from the cryptographic digital signal processor [C-DSP] means to the media ticket smart card with 1st example pass-thru encrypting return means being common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, 2nd example pass-thru encrypting return means being a pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being a row, column table indexed by a vendor identification number, 3rd example pass-thru encrypting return

means being a pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being a row, column table indexed by a vendor identification number,

initializing before playing which is the process done by the customer, party a, of preparing any party's cryptographic media player with his own custom encrypted digital media his own media ticket smart card,

authenticating by customer triangle authentication which is the process done by the cryptographic digital signal processor embedded inside of a cryptographic media player,

transferring of cryptographic keys to the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, by pass-thru encrypting means of cryptographic keys which is the process done by the provided, said new art, cryptographic media player [C-MP] structural means,, to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n transferred over wiretapable computer buses to the player's own provided, said prior art, tamper resistant non-volatile, electrically erasable programmable read-only memory [TNV-EEPROM], for access by its provided, said new art, cryptographic digital signal processor (C-DSP) structural means,

transferring of cryptographic keys away from the provided, said, new art, cryptographic digital signal processor [C-DSP] structural

means, by pass-thru encrypting return means of cryptographic keys which is the process done by the provided, said new art, cryptographic media player's [C-MP's], contained, the cryptographic digital signal processor [C-DSP] structural means, used to transfer encrypted play codes with header and encrypted play counts with header, both having the cryptographic digital signal processor [C-DSP] structural means, incremented sequence counts, transferred to the given, provided, said media ticket smart card a, transferred over wiretapable computer buses,

authenticating using media triangle authentication which is the process of matching the unique digital media with its matching unique play code by the method done by a provided, said new art, cryptographic media player, by using digital media triangle authentication, using sample reads of test data with successful decryption,

cryptographing using hybrid key cryptography which is the process done by a provided, said new art, cryptographic digital signal processor [C-DSP] structural means, inside of a provided, said new art, cryptographic media player [C-MP] structural means,, using provided, said prior art, hybrid key cryptography, which is the process of using the hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys (ssk-n), used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own tamper

resistant, non-volatile memory (TNV-EEPROM) embedded on his black, cryptographic computing unit in the example of a prior art cryptographic digital signal processor (C-DSP) means and a cryptographic central processing unit (C-CPU) which said session keys may be later stored in tamper resistant non-volatile memory (TNV-EEPROM) embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts,

accounting by the provided, said cryptographic digital signal processor [C-DSP] structural means, which is the process done by the cryptographic media player using hybrid key cryptography digital media playing of one-way transfer of custom session key encrypted digital media owned by party n in a controlled access manner mostly for financial accounting purposes which uses the play codes (session key or one-time secret key) and play counts (paid for number of plays or count of free trial plays) contained in media ticket smart cards,

playing by the cryptographic digital signal processor (C-DSP) means which is the process done by the cryptographic media player using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or one-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor (C-DSP) means and also the double secret key decryption of first a unique customer session key decryption followed by a unique vendor secret key decryption used directly used upon the custom encrypted one-way transfer of custom session key encrypted

digital media which is pre-unique vendor secret key encrypted with sequence number checks for countering recorded replay attacks,

escrowing retrieval of lost, stolen, or disputed legal ownership media ticket smart cards, as well as custom cipher text digital media distribution material, which is the process done by the customer, party a, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of 'de facto,' and then internationally standardized cryptography sanctioned by industry trade groups such as the Recording Industry of America Association (RIAA), the Secure Digital Music Initiative (SDMI), the US National Association of Broadcasters (NAB),

whereby this present invention has implemented through the minimal said 3-layer federated system of cryptographic layers of the relevant patent drawing, while for the purposes of this patent process, counting a relevant patent drawing's, combined 2 middle layers of the relevant patent drawing into a single claims layer, comprising of a: low-middle layer for commercial hardware vendors and a high-middle layer for commercial digital media vendors, furthermore, implementing by this process, an assumed design rule of having no inherent hardware and firmware secrecy, no hidden wiretapping points, and also no double key spaces, furthermore, the 4 relevant patent drawing layers, only said drawing's middle 2 layers, condensed into 1 layer for process patent claims broadest purposes, claiming a minimal said 3-layer federated

system of cryptographic process layers by combining the relevant patent drawing's 2 middle-most layers: the bottom-most relevant patent drawing layer or the highest cryptographic system architecture abstraction layer of said system keys under said system party s, in which this system party s's administration through said whole key generation party g, who has been given 100% whole key knowledge, but, 0% knowledge of customer identifications, furthermore, party s also having said whole key distribution party d, who has been given 0% whole key knowledge, but, 100% knowledge of customer identifications [ID's], who has been administer of provided, said cryptographic digital signal processor [C-DSP] structural means, plus any additional, provided, said cryptographic integrated circuit classes [C-IC] structural means, in a industry secret and restricted, hardware distribution process, which has enabled a few trusted national commercial, cryptographic hardware vendors at the bottom-most system layer of party s, of the relevant patent drawing, who are the provided, said, new art, cryptographic digital signal processor [C-DSP] structural means, and provided, said prior art, smart card, hardware vendor parties, s, being the bottom-most layer for this process patent claim, who are legally allowed or trusted, by party d, to firmware program with confidential system cryptographic keys, said tamper resistant non-volatile memory (TNV-EEPROM) of each said cryptographic integrated circuit classes [C-IC] and also said smart cards, in order to keep said system keys top secret, furthermore, at the 2nd from bottom-most relevant patent drawing layer, of system hardware world-wide distribution vendors, parties vn, under administration of said party d, said PC cryptographic hardware plug-in board classes of hardware vendors, are simply given by said

system authority distribution party d, 100% pre-programmed with cryptographic system keys, said, tamper resistant non-volatile memory [TNV-EEPROM] which is pre-stored inside of centrally distributed, said cryptographic integrated circuit device classes [C-IC's], used to install in their PC peripheral device hardware, furthermore, at the 3rd from bottom cryptographic layer of the relevant patent drawing or high-middle layer of this process patent claim, of said party d administered, digital media distribution vendor parties vn, the cryptographic layer of commercial system administrators having vested commercial interests with their own commercial industry groups, furthermore, at the said parties vn administered, top-most relevant patent drawing's, cryptographic architecture layer of said customer parties: a, b, c, i to z, and his given, unique per customer party a, only said smart card a, distributed and securely protected by provided, said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], cryptographic keys, are known only to the highly federated high-middle vendor or key industry layers of commercial, split key escrow databases, alltogether implementing a highly federated cryptography system,

whereby the present invention has created, several processes for doing unique, customer custom session key or one-time secret key encrypted copies of initially unique, vendor secret key encrypted, digital media distribution over the prior art, insecure ('red bus') Internet using secure, World Wide Web (WWW) ('black') servers involving the cryptographically secure transfer ('download') from Web server to customer prior art, personal computers (PC's) over insecure ('red bus')

Internet connection lines, of custom encrypted, digital media to prior art, standard form recordable media, and also custom decryption cryptographic keys ('play codes') and custom pre-programmed accounting counts ('play counts') for deposit onto prior art, smart cards called media ticket smart cards,

whereby the present invention has created, several processes for securely physically transferring ('footprint download') of both said custom, encrypted digital media on standard form recordable media along with the customer's universal media ticket smart card for all vendors and all digital media to said cryptographic media players having embedded pre-programmed prior art, said cryptographic digital signal processors (C-DSP's) for media playing which are universally and uniquely, pre-programmed for every authorized vendor participating in the system, and can also accept any authorized, unique customer's smart card which must have relevant play codes and play counts for upload and use which are both uniquely matched to the authorized custom encrypted digital media inserted for playing,

whereby this present invention has achieved, a highly federated or regional cryptography architecture is commercially implemented by commercial industry organizations, proximately in human corporate organization, corresponding to today's US based, prior art, magnetic strip credit card management and distribution industry group associations, with corresponding EU based prior art, smart card commercial corporate organizations, furthermore, implementing through the process of this patent, over the global Internet-Web, individual human level and corporate body human level, trust granting policies

known as a relative, two-way, middle level individual-organizational trust granting model, or a middle level trust model, versus, earlier highly centralized, 100% top-down trust granting models exampled by the US Federal National Institute of Standard's (NIST's) Clipper chip and Capstone program, versus, earlier 100% bottom-up trust granting models, often called tangled web of trust models,

whereby this present invention has allowed, using several of the above systems processes in safeguarding relative, commercial value, of multi-million dollar digital masters released by vendors through World Wide Web (WWW) distribution.

96. (NEW) The process of claim 95 whereby the method or process of cryptographing using public key cryptography which is the process done by said cryptographic media player with its embedded said cryptographic digital signal processor [C-DSP] structural means, using public key cryptography which is the process of using public key cryptography authentication, encryption, and decryption using public keys (puk-n), and private keys (prk-n), stored within tamper resistant non-volatile memory (TNV-EEPROM) embedded within non-wiretapable ("black") cryptographic computing units in the example of cryptographic digital signal processors (C-DSP) means,

whereby this process has implemented, a very low probability of hacker intercept, provided, said prior art, public key cryptography algorithms inside of provided, said cryptographic media players [C-MP] structural means, hardware computing units, achieving unique remote party public key authentication, and also relatively very slow execution speeds, public key encryption.

97. (NEW) The process of claim 95 whereby the process or method of cryptographing using secret key cryptography which is the process done by said cryptographic media player with its embedded said cryptographic digital signal processor [C-DSP] structural means, using secret key cryptography which is the process of using secret key cryptography with a non-wiretapable ["black"] bus, cryptographic computing unit in example of a cryptographic digital signal processing (C-DSP) means using secret keys [SeK-N], or session keys [SsK-N], stored upon tamper resistant, non-volatile memory [TNV-EEPROM], consists of the sub-step of:

cryptographing using fast hardware session key cryptography which is the process done by a cryptographic digital signal processor [C-DSP] means inside of a cryptographic media player using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ("black"), cryptographic digital signal processing [C-DSP] means with access to higher level tamper resistant non-volatile ["black"] memory for cryptographic key storage of private keys and secret keys, which hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key cryptography encryption and decryption of block transferred digital media,

whereby this process has implemented a very fast executing, provided, said prior art, secret key encryption algorithm, inside of provided, said new art, cryptographic media players [C-MP] structural means, versus a typically much slower in execution speed in both hardware and add-on software, provided, said prior art, public key cryptography algorithm, both being combined at higher process levels in hybrid key cryptography.

==========

98. (NEW) A specific process for doing public key cryptography over an open systems architecture in a relatively commercial level secure, cryptographically secure manner, meant for safeguarding relative commercial value, multi-million dollar digital masters for the specific process of "over the air," broadband cable, broadband phone line, direct digital satellite, or Institute of Electrical and Electronic Engineers [IEEE], wireless Ethernet distribution, only structural means exampled by IEEE 802.11 b/c/g, of custom pre-encrypted, 'custom cipher text,' digital media distribution custom download into a new art, cryptographic set-top box, and also group broadcast of pre-encrypted 'custom cipher text,' in high definition television [HDTV] or a lower band-width subset of standards definition television [SDTV] digital form, into the same new art, cryptographic set-top box, which open systems architecture includes existing prior art components integrated into a new art systems process of:

providing of the component of: prior art, a tamper-resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], with means for tamper resistant permanent memory storage,

providing of the component of: a static random access memory [SRAM], with means for non-permanent solid state memory storage,

providing of the component of: prior art, a dynamic random access memory [DRAM], with means for volatile solid state memory storage,

providing of the component of: prior art, a cryptographic micro-controller [C-u-Ctlr], with means for secure storage of cryptographic keys in contained, provided, said prior art, tamper resistant non-volatile permanent memory [TNV-EEPROM], plus other cryptographic hardware aids for strong cryptography,

providing of the component of: prior art, a smart card used for media ticket applications containing provided, said prior art, cryptographic, embedded micro-controller's [C-u-Ctlr's], furthermore, already having contained, provided, said prior art, tamper resistant, non-volatile electrically erasable programmable read-only memory [TNV-EEPROM] for key storage,

providing of the component of: new art, a cryptographic smart card with bio-ID, used for media ticket applications containing provided, said prior art, cryptographic embedded, micro-controller [C-u-ctlr], as well as containing provided, said prior art, tamper resistant, non-volatile memory [TNV-EEPROM] for key storage, as well as containing in crypto-memory the embedded bio-ID in some digital form, of the unique smart card owner,

providing of the component of: prior art, serial data computer communications interfaces,

providing of the component of: prior art, a smart card reader, with means for reading said smart card,

providing of the component of: prior art, biological-identification readier [bio-ID reader] means which attach to personal computers [PC's], with bio-ID means such as: digitized fingerprint readers, digitized iris scan readers, digitized facial cognitive features readers, digitized DNA readers.

providing of the component of: prior art, an internet protocol [IP], wide area network [IP WAN],

providing of the component of: prior art, a world wide web server [WWW] or web or graphics rich portion of the Internet web server computer,

providing of the component of: prior art, a personal computer [PC], which is non-cryptographically secure,

providing of the component of: prior art, a personal computer [PC] web client,

providing of the component of: prior art, a personal computer [PC] peripherals,

providing of the component of: prior art, a data entry devices of an on-board protected electronic device, toggle field with a prior art liquid crystal display [LCD] for entry of the unique customer passphrase with closely corresponding passcode entry,

providing of the component of: prior art, a data entry device of computer keyboards,

providing of the component of: provided said, new art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-text data sent to an attached provided, said prior art, digital serial bus, furthermore, 1st example means being digitized fingerprint bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of: prior art, a banked-EEPROM card reader-writer,

providing of the component of: prior art, a personal computer's [PC's] peripheral data storage devices, with means for detachable or removable non-volatile memory units,

providing of the component of: prior art, a personal computer's [PC's] based peripheral data storage media units, with means for archival storage of large amounts of digital data,

providing of the component of: prior art, a digital signal processor [DSP],

providing of the component of: a new art, a cryptographic digital signal processor [C-DSP], furthermore, having functional means for secure cryptographic key storage through contained, provided, said prior art, tamper resistant non-volatile memory [TNV-EEPROM],

providing of the component of: new art, cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through contained, provided, said prior art, tamper resistant non-volatile memory [TNV-EEPROM], furthermore, through enhanced cryptographic hardware aids for both secret key and for public key, strong cryptography,

providing of the component of: a new art, programmable gate array logic [GAL] form of high density, application specific integrated circuit [ASIC] with embedded, provided, said cryptographic digital signal processor [C-DSP] structural means, functions as mentioned in the paragraph just above,

providing of the component of: a new art, cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through contained, provided, said prior art, tamper resistant non-volatile memory [TNV-EEPROM], furthermore, through enhanced strong cryptographic algorithm, hardware aids, for both secret key and for public key, strong cryptography, furthermore, with hardware and firmware support for modern secret key ciphers such as the Advanced Encryption Standard [AES] cipher stressing variable length secret key strength,

providing of the component of: prior art, a non-cryptographic micro-processor [uP] or a central processing unit [CPU], with exampled implementation means such as a commercial, 32-bit, Intel Pentium class of micro-processor central processing unit [CPU], with a control unit and on-chip floating point processing unit,

providing of the component of: a new art, a cryptographic computing micro-processor [C-uP] based unit, furthermore, having a hardware design implementation of a proper subset or silicon compiler class library selection, of said cryptographic micro-controller [C-u-CTLR], with means for secure handling of strong cryptography keys and auxiliary strong cryptography hardware aids,

providing of the component of: a new art, a cryptographic computing micro-processor [C-uP] based unit, furthermore, having a hardware design implementation of a proper subset or silicon compiler class library selection, of said cryptographic digital signal processing [C-DSP] structural means, furthermore, having structural means for secure handling of strong cryptography keys intended for commercial digitally compressed, digital music and movies,

providing of a new art, class of cryptographic computing hardware integrated circuit [C-IC] units containing the proper subset, functionality of the provided, said new art, cryptographic digital signal processor [C-DSP] structural means, comprising of the above exampled, cryptographic digital signal processor [C-DSP] structural means, plus very similar in hardware design given modern grey scales of very cost competitive, digital chip architectures, ranging in

relevance, from design bench, custom fuse link programmable, application specific integrated circuits [ASIC'S], all the way in grey scale digital computing complexity, to modern silicon compiler custom designed integrated circuits [IC's] for mass production, as structural implementation hardware means, only illustrated by the above cryptographic hardware units, with functional means for keeping strong cryptography: secret keys, private keys, family keys, session keys, and often used public keys, secret in secure tamper resistant hardware or red-black hardware, including as a component, said tamper resistant, non-volatile electrically erasable read only memory [TNV-EEPROM], with means of using pass-thru encryption methods over open or wiretapable digital computer system buses to confidentially and securely, transfer said strong cryptography keys into the said hardware from an external wiretapable, input-output serial bus connected source only exampled by a human portable vault functional means, structural means of a smart card, and its own said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], furthermore, also exampled by a remote local area network [LAN] source, furthermore, also exampled by a MODEM connected remote global Internet-Web source,

providing of the component of: a prior art, media player [MP], having internal, provided said prior art, digital signal processors [DSP's],

providing of the component of: a new art, a cryptographic media player [C-MP], constructed with a provided said, new art, cryptographic digital signal processor [C-DSP] structural means, having structural means for internal provided said, prior art, tamper resistant non-volatile, electrically erasable programmable read only memory [TNV-EEPROM], for playing of customized per customer, strong encrypted digital media,

providing of the component of: a new art, cryptographic media player [C-MP], with means for playing back custom secret key encrypted, compressed digital, audio-video in standard format,

providing of the component of: a new art, cryptographic personal computer [C-PC] which is created by using provided, said new art, said cryptographic micro-processor [C-uP], with structural means for digitally processing, new art, custom encrypted digital media,

providing of the component of: a new art, cryptographic personal computer [C-PC] having a subset functionality of provided, said new art, cryptographic micro-processor [C-uP], which is created by using a prior art, standard off-the shelf, personal computer [PC] design with a provided, said new art, cryptographic micro-processor unit [C-uP],

providing of the component of: provided said, new art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-

text data sent to an attached provided, said prior art, digital serial bus, furthermore, attached to a provided, said new art, cryptographic PC [C-PC], furthermore, 1st example means being digitized fingerprint bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of a new art, cryptographic operating system [C-OS], designed for provided said, new art, cryptographic micro-mirror module (C-MMM), having an internal provided said, cryptographic micro-processor unit (C-uP),

providing of the component of: new art, a universal cryptographic set-top box, form of provided said, cryptographic media players [C-MP's] structural means, for playing back customized digital media,

providing of the component of: a new art, cryptographic micro-mirror module [C-MMM], commercial theater projection-theater sound units which are special cryptographic personal computers [C-PC's] structural means, furthermore, which use prior art, removable permanent memory devices,

providing of the component of: prior art, a modified secure operating system [secure-OS] for world wide web [WWW] server computers which will custom customer session key encrypt a vendor secret key encrypted digital master, and electronically distribute custom, encrypted digital media masters, using firewalls, using anti-viral software updated weekly, using network protocol converters, using standard layered security methods, and using 'inner sanctum' protection for vendor session key or one-time secret key encrypted digital media masters,

providing of the component of: prior art, a global Internet and world wide web [WWW] based transmission control protocol-internet protocol [TCP-IP] command protocol stack program for Internet connectivity,

providing of the component of: prior art, standard, a plurality of cryptographic mathematics algorithms,

providing of the component of: prior art, a plurality of public key cryptography algorithms which create public keys and private keys,

providing of the component of: prior art, a plurality of secret key cryptography algorithms which create secret keys and session keys or 1-time use only, secret keys, and also play counts or access counts or media decryption counts and play codes or session keys or 1-time use only secret keys,

providing of the component of: prior art, a plurality of hybrid key cryptography algorithms which are combined public key and private key cryptography algorithms,

providing of the component of: prior art, a plurality of private key and secret key splitting algorithms,

providing of the component of: prior art, a plurality of private key and secret key escrow techniques,

providing of the component of: prior art, a plurality of algorithms used to generate: cryptographic keys which are the collective public keys, private keys, secret keys, session keys or 1-time use only secret keys, play counts, play codes, passphrases-passcodes,

providing of the component of: prior art, a plurality of computer cryptography protocols,

providing of the component of: prior art, a plurality of pass-thru encryption algorithms for transmitting secure data over wiretapable computer buses ['red buses'],

providing of the component of: prior art, standardized form, a plurality of lossy compressed digital media algorithms with many prior art example means, and new art emerging future standards,

providing of the component of: prior art, a transmissions control protocol/internet protocol [TCP/IP] for Internet connectivity,

providing of the component of: prior art, a secure internet protocol layer [secure IP layer] layer of Internet data encryption, used in this present patent only as an outer-most security layer which is considered cryptographically un-reliable,

providing of the component of: prior art, a secure sockets layer [SSL] layer of Internet data encryption,

providing of the component of: prior art, a plurality of world wide web [WWW] server standard interchange file language with 1st example protocol being hyper-text mark-up language [HTML], 2nd example protocol being extensible business mark-up language [XBML] also known as [XML], and third example protocol being the most generalized-text mark-up language [GTML],

providing of the component of: a plurality of world wide web [WWW] client standard interchange file languages, with 1st example being hyper-text mark-up language [HTML],

generating of a set of common system keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using provided prior art said public key and secret key cryptography algorithms to generate system cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding of generated said common system keys into each and every provided, said cryptographic digital signal processor [C-DSP]

structural means, and also if relevant, a provided said cryptographic integrated circuit [C-IC], furthermore, embedding said common system keys into the said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM] inside of each and every, provided said smart card,

generating of a set of unique per vendor, commonly distributed only in provided, said tamper resistant hardware [TNV-EEPROM], media distribution vendor cryptographic keys eventually used in a provided said, new art, cryptographic digital signal processor [C-DSP] structural means, and also if relevant, a provided said, new art,, cryptographic integrated circuit [C-IC], involving several processes with a 1st example prior art, provided, said, being the US National Institute for Standards and Technology's Clipper-Capstone chip with provided, said embedded tamper resistant non-volatile electrically erasable programmable read-only memory (TNV-EEPROM), and a 2nd example provided said, new art, cryptographic digital signal processor (C-DSP) structural means, being a prior art, digital signal processor having a silicon compiler designed equivalent of the former's functions [C-DSP] structural means, with added silicon compiler functions for prior art algorithm means for subsequent customer uses of digital signal compression audio-video digital compression means involving several processes and components with 1st example audio-video digital compression means involving several processes being given as prior art, Moving Picture Electronics Group standards X [MPEG X], 2nd example audio-video digital compression means being given as prior art, fast wavelet audio-video compression or

convolutional coding compression, 3rd example audio only digital compression example means being given as prior art, MPEG I audio layer 3 [MP3], and 4th example audio only digital compression example means being given as prior art, fast wavelet audio only compression algorithms [AAC], furthermore, with subsequent customer uses of a prior art, pass-thru encryption means involving several processes and components which are used to transfer said unique customer cryptographic keys over wirctapablc or opcn computcr buscs ['rcd buses'] with a first example pass-thru encryption means given as common, family key, secret key encryption, a second example pass-thru encryption means given as common family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor public keys followed by the relevant vendor public key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor public keys followed by relevant vendor private key decryption of the received data block, and a third example pass-thru encryption means being a family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor secret keys followed by the relevant vendor secret key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor secret keys followed by relevant vendor secret key decryption, for eventual manufacturing into a cryptographic media player, which is the process done by the media ticket smart card system authority's, party s's, dedicated

public key generation authority, party g, using prior art algorithms for both public key and secret key cryptography to generate a unique set of vendor cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding in entirety, said unique set of vendor cryptographic keys in an organizational table form means involving several processes with 1st example organizational table form means being a unique vendor system key table which is indexed by a vendor identification number, furthermore, said organizational table form means is semi-conductor foundry factory embedded into each and every provided, said new art, cryptographic digital signal processor [C-DSP] structural means, while specific vendor private keys and vendor secret keys including a minimum count of one vendor key of the private key of vendor party vn, are factory time embedded into each and every one of vendor party vn's eventually distributed provided, said media ticket smart cards and their internal, provided, said prior art, cryptographic micro-controller [C-u-Ctlr], for use in a pass-thru encryption means of several example pass-thru encryption means as explained in a separate process,

generating of a unique media ticket smart card cryptographic key set or also known as a given, unique customer party a's, chosen out of the unique customer party's: a, b, c, i to z's, cryptography key set, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using provided, prior art algorithms for both public key and secret key cryptography to generate unique customer cryptographic

keys, while having absolutely no access to customer identifications, furthermore, the sub-process of embedding into a provided, single said unique media ticket smart card with an embedded cryptographic micro-processor [C-uP], a unique customer party a's, unique cryptographic key into party a's, eventually distributed provided, said media ticket smart card with its internal cryptographically secure storage of provided, said embedded cryptographic micro-processor [C-uP],

distributing of provided, said cryptographic digital signal processor [C-DSP] structural means, furthermore, the distributing of said cryptographic digital signal processor [C-DSP] structural means is based upon the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing provided, said cryptographic digital signal processor [C-DSP] structural means to individual media distribution vendors for manufacturing into vendor party vn's cryptographic media players while having absolutely no access to whole cryptographic keys and having unique vendor party vn access to only his own unique vendor secret key vn, and unique vendor private key vn, with its unique, matching public key vn,

distributing of the factory cryptographically programmed, provided, said media ticket smart cards, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys,

escrowing of the split cryptographic keys which is the process done by the central public key generation authority, party g, safe-guarding the split cryptographic customer keys, and split cryptographic vendor keys in an entirely secure and confidential manner for achievement of legal means involving several processes, with a 1st example legal means being simple customer identification and lost cryptographic key recovery, a 2nd example legal means being court ordered only, disputed ownership cryptographic key recovery, and a 3rd example legal means being court ordered only cryptographic key recovery use by law enforcement,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with a minimum of 3-layers of digital computer architecture: a lowest relevant patent drawing layer, composed of the media ticket smart card system authority, a middle layer composed of authorized media distribution companies labeled as parties vn, and a highest layer or user or customer parties: a, b, c, i to z, layer composed of customers,

preparing of a unique play code and a unique play count which is the process done by the authorized digital media distribution unique vendor company, party vn, preparing said unique play code [a session key or one-time use secret key], and said unique play counts [a paid for number of plays or count of free trial plays], and preparing of the custom encrypted digital media for downloading to each customer,

downloading to unique customer party, a, b, c, i to z, at a private dwelling, prior art, insecure ('red bus'), personal computer [PC] which is the process done by the authorized digital media distribution vendor, party vn, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a prior art, provided, world wide web [WWW] server over the global Internet to multiple prior art, provided, personal computer [PC] based web clients, one of whom is customer party, a, b, c, or i to z, of encrypted play codes (one-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into said factory cryptographically programmed, prior art, provided, media ticket smart cards attached to prior art, provided, personal computer (PC based) media ticket smart card readers, and one-way transfer of custom session key or one-time use only secret-key encrypted pre-unique vendor secret key encrypted digital media for deposit into physical digital media inserted into media drives attached to prior art, provided, customer personal computers (PC's),

delivering by foot which is the process done by the given, unique customer party a, of physically transferring both physical custom encrypted digital media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, prior art, provided, personal computer [PC] to any other customer party's: a, b, c, i to z, provided, said cryptographic media player [C-MP] structural means,, with its embedded said cryptographic digital

signal processor [C-DSP] structural means, also with a built-in media ticket smart card reader,

encrypting in a pass-thru manner for media ticket smart card upload to a provided said, new art, cryptographic media player [C-MP] structural means, structural means, with its internal, provided, said cryptographic digital signal processor [C-DSP] structural means, using pass-thru encrypting means involving several processes and components for transferring any type of digital data securely from originating said media ticket smart card up to answering provided, said cryptographic digital signal processor [C-DSP] structural means, with a 1st example pass-thru encrypting means being said common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, a 2nd example pass-thru encrypting means being originate vendor, unique, vendor private key digital signaturing to 'signatured-text' or not encrypted text thus readable by any party, furthermore, followed by answering vendor, unique, vendor public key digital public key encryption to 'cipher-text' or encrypted text, furthermore, using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being a row, column table indexed by a vendor identification number, a 3rd example pass-thru encrypting means being originate vendor, unique, vendor secret key encryption to 'cipher-text (encrypted text which combines signaturing)' using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with

first organizational means being a row, column table indexed by a vendor identification number,

encrypting in a pass-thru return manner for provided, said new art, cryptographic media player's [C-MP] structural means, contained, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, download to said media ticket smart card, by using pass-thru encrypting return means involving several processes and components for transferring any type of digital data securely from provided, said new art, cryptographic digital signal processor [C-DSP] structural means, to said media ticket smart card, with a 1st example pass-thru encrypting return means being common family key or shared secret key encryption which is known vulnerable to a single point of failure, 2nd example pass-thru encrypting return means being answer vendor unique private key digital signaturing to 'signatured-text' or digitally signatured text which is non-encrypted, and thus readable by any party, followed by originate vendor unique public key encryption to 'cipher-text' or encrypted text using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being the row, column table indexed by a vendor identification number, a 3rd example pass-thru encrypting return means being answer vendor unique secret key encryption to 'cipher-text' or encrypted text, which combines digital signaturing by using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational

means being the row, column table indexed by a vendor identification number,

initializing before playing which is the process done by the customer, party a, of preparing any customer party's: a, b, c, i to z, personally owned provided, said cryptographic media player, with its internal, provided, said cryptographic digital signal processor [C-DSP] structural means, by inserting his own party a's unique custom encrypted digital media, and also by inserting his own party a's unique provided, said media ticket smart card,

transferring of the cryptographic keys from the prior art, provided, said media ticket smart card to provided said, new art, cryptographic media player having its prior art, provided, embedded said cryptographic digital signal processor (C-DSP) structural means, by use of said pass-thru encrypting means, of the unique customer cryptographic keys over wiretapable or open computer buses ('red buses') which is the process done by the cryptographic media player to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n which are pass-thru encrypted by the several pass-thru encryption means involving several processes and components for transfer over wiretapable computer buses ('red buses') to the player's own cryptographic memory (TNV-EEPROM) for access by its cryptographic digital signal processor (C-DSP) means, with said 1st example pass-thru encryption means being the common family key encryption vulnerable to a single point of attack, a said 2nd example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys

which uses a family key encrypted, common table index for efficient active table entry access, a said 3rd means of pass-thru encryption being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access,

transferring of the cryptographic keys away from provided said, new art, cryptographic media player having its embedded said cryptographic digital signal processor (C-DSP) means to said media ticket smart card by pass-thru encrypting return means of the unique customer cryptographic keys over wiretapable or open computer buses ('red buses') which is the process done by the cryptographic media player which are pass-thru encrypted by the several pass-thru encryption means for transmit using it's cryptographic digital signal processor (C-DSP) means, the encrypted play codes with header and encrypted play counts with header both with cryptographic digital signal processor (C-DSP) means incremented sequence counts (to avoid recorded replay attacks without the use of synchronized digital clocks) to the media ticket smart card A transferred over wiretapable computer buses, with said 1st example pass-thru encryption means being the common family key encryption vulnerable to a single point of attack, a said 2nd example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said 3rd means of pass-thru encryption being the unique vendor secret key encryption

with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access,

authenticating using media triangle authentication which is the process of matching the unique digital media with its matching unique play code by the method done by said cryptographic media player's embedded said cryptographic digital signal processor doing digital media triangle authentication using sample reads of test data with successful decryption,

cryptographing using hybrid key cryptography which is the process done by the provided, said new art, cryptographic media player's [C-MP's] embedded provided, said cryptographic digital signal processor [C-DSP] structural means, using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys [ssk-n], used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own provided, said tamper resistant, non-volatile memory [TNV-EEPROM] embedded on his provided, said cryptographic digital signal processing [C-DSP] structural means, with a 1st example means of the provided said, new art, cryptographic digital signal processor [C-DSP] structural means, and a 2nd example means of a provided, said cryptographic integrated circuit [C-IC], which said 1-time use only secret keys or session keys, may be later stored in provided, said tamper resistant non-

volatile memory [TNV-EEPROM], embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts,

accounting by provided said cryptographic media player's embedded, provided, said cryptographic digital signal processor [C-DSP] structural means, which is the process done using hybrid key cryptography digital media playing of one-way transfer of custom session key encrypted digital media, owned by unique customer party a, in a controlled access manner mostly for financial accounting purposes which uses the play codes [session key or one-time secret key] and play counts [paid for number of plays or count of free trial plays] contained in media ticket smart cards,

playing by provided, said cryptographic media player having its embedded, provided, said cryptographic digital signal processor [C-DSP] structural means which is the process done using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or one-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor (C-DSP) means and also the hardware secret key double decryption directly used upon the custom encrypted, one-way transfer of custom session key encrypted digital media which is pre-unique vendor secret key encrypted, using first the unique customer session key decryption and then the unique vendor secret key decryption with sequence number checks for countering recorded replay attacks,

viewing of electronic television guide [e-TV guide] picture in a picture [PIP] viewing and channel selection and future program recording such as through an example graphical user interface (GUI) means of a "spreadsheet type" or "matrix type" of display, which can easily be removed in a MPEG X decompression circuit as very low digital bandwidth, MPEG X annotation data, for sending to video RAM and subsequent display in a digital picture in a picture (PIP) on a digital monitor,

custom broadcasting to given customer, party a, which is the process done by the authorized digital media distribution vendor, party vn, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a broadcast server to multiple homes or businesses having cryptographic set-top boxes for one-way transfer of custom session key encrypted digital media for possible digital recording into physical digital media inserted into media drives attached to an attached digital recorder,

escrowing retrieval of lost, stolen, or disputed legal ownership media ticket smart cards, as well as custom cipher text digital media distribution material, which is the process done by the unique customer, party a, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of 'de facto' industry standards, leading to internationally standardized cryptography sanctioned by industry trade groups such as the Recording Industry Association of America's [RIAA's] Secure Digital

Music Initiative [SDMI], the National Association of Broadcaster's [NAB's] Secure Digital Broadcast Group [SDBG],

whereby the present invention has implemented through the minimal said 3-layer federated system of cryptographic this claim's layers, while counting as one for this claims purposes, a combined, a relevant patent drawing's 2 middle of 4 layers, comprising of: the relevant patent drawing into a low-middle layer for commercial hardware vendors and a high-middle layer for commercial digital media vendors, a process implemented design rule of having no inherent hardware and firmware secrecy, no hidden wiretapping points, and also no double key spaces, furthermore, the minimal said 3-layer federated system of cryptographic layers of this invention's this claim's layers: the bottom-most relevant patent drawing's cryptographic system architecture layer of said system keys under said system party s, in which this system party s's administration through said whole key generation party q, who has been given 100% whole key knowledge, but, 0% knowledge of customer identifications, furthermore, party s also having said whole key distribution party d, who has been given 0% whole key knowledge, but, 100% knowledge of customer identifications [ID's], who has been administer of provided, said cryptographic integrated circuit [C-IC] classes, hardware distribution process, which has enabled only a few trusted national commercial, cryptographic hardware vendors who are legally allowed by party d, to firmware program with confidential system cryptographic keys, said tamper resistant non-volatile memory (TNV-EEPROM) of each said cryptographic integrated circuit classes [C-

IC], in order to keep said system keys top secret, furthermore, at the relevant patent drawing's, low-middle level layer of system hardware world-wide distribution under administration of said party d, said PC cryptographic hardware plug-in board classes of hardware vendors, are simply given by said system authority distribution party d, 100% pre-programmed with cryptographic system keys, said, tamper resistant non-volatile memory [TNV-EEPROM] which is pre-stored inside of centrally distributed, said cryptographic integrated circuit device classes [C-IC's], used to install in their PC peripheral device hardware, furthermore, at the relevant patent drawing's high-middle cryptographic layer of said party d administered, digital media distribution vendor parties vn, the cryptographic layer of commercial system administrators having vested commercial interests with their own commercial industry groups, furthermore, desirably aided in commercial secrets enforcement by future, commercial anti-espionage felony laws, furthermore, at the relevant patent drawing's, top-most, cryptographic layers of said high-middle digital media distribution parties vn, administered, customer parties: a, b, c, i to z, and given customer a and his unique per customer, only said smart card a, distributed and securely protected by said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], cryptographic keys, are known only to the relevant patent drawing's, high-middle claim's layer of digital media distribution vendor parties vn, contained within secure, optional by dependent claim, key industry layers of commercial, split key escrow databases, alltogether implementing a highly federated cryptography system,

whereby the present invention has created several processes for doing unique, customer custom session key or one-time secret key encrypted copies of initially unique, vendor secret key encrypted, digital media distribution over the prior art, insecure ('red bus') Internet using secure, World Wide Web (WWW) ('black') servers involving the cryptographically secure transfer ('download') from Web server to customer prior art, personal computers (PC's) over insecure ('red bus') Internet connection lines, of custom encrypted, digital media to prior art, standard form recordable media, and also custom decryption cryptographic keys ('play codes') and custom pre-programmed accounting counts ('play counts') for deposit onto prior art, smart cards called media ticket smart cards,

whereby the present invention has created several processes for securely physically transferring ('footprint download') of both said custom, encrypted digital media on standard form recordable media along with the customer's universal media ticket smart card for all vendors and all digital media to said cryptographic media players having embedded pre-programmed prior art, said cryptographic digital signal processors (C-DSP's) for media playing which are universally and uniquely, pre-programmed for every authorized vendor participating in the system, and can also accept any authorized, unique customer's smart card which must have relevant play codes and play counts for upload and use which are both uniquely matched to the authorized custom encrypted digital media inserted for playing,

whereby this invention has created a highly federated or regional cryptography architecture, which has been commercially implemented by

commercial industry organizations, proximately in human corporate organization, corresponding to today's US based, prior art, magnetic strip credit card management and distribution industry group associations, with corresponding EU based prior art, smart card commercial corporate organizations, furthermore, implementing through the process of this patent, over the global Internet-Web, individual human level and corporate body human level, trust granting policies known as a relative, two-way, middle level individual-organizational trust granting model, or a middle level trust model, versus, earlier highly centralized, 100% top-down trust granting models exampled by the US Federal National Institute of Standard's (NIST's) Clipper chip and Capstone program, versus, earlier 100% bottom-up trust granting models, often called tangled web of trust models,

whereby this present invention has implemented, with future planning using Moore's Law of industrial engineering in semi-conductor device fabrication is reasonable compensated, especially regarding future expansions in capacity of provided, said tamper resistant non-volatile, electrically erasable programmable read-only memory [TNV-EEPROM],

whereby this present invention has achieved, using several of the above systems processes in safeguarding relative, commercial value, of multi-million dollar digital masters released by vendors through global World Wide Web (WWW) distribution.

99. The process of claim 98 whereby the process of authenticating by customer triangle authentication, which is the process done by the 3 geometric points of: point 1: provided said, new art, smart card with bio-ID, point 2: given customer party a of customer parties: a, b, c, i to z, and point 3: an authorized provided, said new art, cryptographic media player [C-MP] structural means, with its provided, said new art, cryptographic digital signal processor [C-DSP] structural means, furthermore, which process step may be skipped for low security only when customer time and effort is of the essence,

whereby this process claim has achieved, a highly efficient and high probability, uniqueness of a minimum of 3 involved, parties n, in verifying the given customer party a, out of customer parties: a, b, c, i to z, to both the provided, said smart card inserted, and only authorized provided, said new art, cryptographic set-top boxes [C-BOX] in the process called customer triangle authentication.

100. (NEW) The process of claim 98 whereby the process of public key cryptographing is done for authentication by provided, said new art, cryptographic media player [C-MP] structural means, with its provided, said new art, cryptographic digital signal processor [C-DSP] structural means, and also by provided, said new art, cryptographic set-top box [C-BOX] structural means, with its embedded provided, said new art, cryptographic digital signal processor [C-DSP] structural means, using provided said, prior art, public key cryptography algorithms which is the process of using public key cryptography authentication, encryption, and decryption using public keys [puk-n], and private keys [prk-n], stored within provided, said tamper resistant non-volatile memory [TNV-EEPROM] embedded within non-wiretapable ["black"] cryptographic computing units in the example of provided, said new art, cryptographic digital signal processors [C-DSP] structural means,

whereby this process claim has implemented, a very low probability of hacker intercept, provided, said prior art, public key cryptography algorithms inside of provided, said cryptographic set top boxes [C-BOX's] hardware computing units, achieving unique remote party public key authentication, and also relatively very slow execution speeds, public key encryption.

101. (NEW) The process of claim 98 whereby the process of secret key cryptographing uses prior art, secret key cryptography which is the process done by provided, said new art, cryptographic media player [C-MP] structural means, and also by provided, said cryptographic set-top box [C-BOX] with its embedded provided, said new art, cryptographic digital signal processor [C-DSP] structural means, using provided said, prior art, secret key cryptography, which is the process of using provided, said prior art, secret key cryptography with a non-wiretapable ["black"] bus, cryptographic computing unit in structural means, exampled by a provided, said new art, cryptographic digital signal processing [C-DSP] structural means, using 1-time use only secret keys [sek-n] or session keys [ssk-n], stored upon provided, said tamper resistant, non-volatile memory [TNV-EEPROM], using the following sub-process:

cryptographing using fast hardware session key cryptography which is the process done by a provided, said new art, cryptographic digital signal processor [C-DSP] structural means, internal to a provided, said new art, cryptographic set-top box [C-BOX], using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ["black"], provided, said new art, cryptographic digital signal processing [C-DSP] structural means, with access to higher security level, provided, said tamper resistant non-volatile [TNV-EEPROM] ["black"]) memory for

cryptographic key storage of private keys and secret keys, which hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key cryptography encryption and decryption of block transferred digital media,

whereby this process claim has accomplished with a very low probability of hacker intercept, very fast and efficient, execution speed, digital computer execution of provided, said prior art, secret key cryptography algorithms, inside of provided, said new art, cryptographic set-top boxes [C-BOX's].

==========

102. (NEW) A specific process for doing public key cryptography over an open systems architecture in a totally cryptographically secure manner meant for safeguarding relative commercial value, multi-million dollar digital masters, for the process of federated central level, commercial movie distribution to fully digital, new art, cryptographic micro-mirror modules [MMM] in each commercial movie theatre, having several means of global Internet-Web, also warm blooded courier distribution of new art, custom encrypted digital media, which open systems architecture includes existing prior art components to give new art systems processes of:

providing of the component of: prior art, a tamper-resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], with means for tamper resistant permanent memory storage,

providing of the component of: a static random access memory [SRAM], with means for non-permanent solid state memory storage,

providing of the component of: prior art, a dynamic random access memory [DRAM], with means for volatile solid state memory storage,

providing of the component of: prior art, a low-cost, low-throughput, embedded cryptographic micro-controller [C-u-Ctlr], with means for secure storage of cryptographic keys in said tamper

resistant non-volatile permanent memory [TNV-EEPROM] storage, plus other cryptographic hardware aids for strong cryptography,

providing of the component of: prior art, the smart card used for media ticket applications containing tamper resistant, non-volatile memory [TNV-EEPROM] for key storage as part of provided, said prior art, cryptographic micro-controller [C-u-CTLR],

providing of the component of: new art, the smart card with bio-ID, used for media ticket applications containing tamper resistant, non-volatile memory [TNV-EEPROM] for key storage as part of provided, said prior art, cryptographic micro-controller [C-u-CTLR], furthermore, containing in the crypto-memory a unique card owners bio-ID,

providing of the component of: prior art, serial data computer communications interfaces,

providing of the component of: prior art, a smart card reader, with means for reading said smart card,

providing of the component of: prior art, biological-identification readier [bio-ID reader] means which attach to personal computers [PC's], with bio-ID means such as: digitized fingerprint readers, digitized iris scan readers, digitized facial cognitive features readers, digitized DNA readers.

providing of the component of: prior art, an internet protocol [IP], wide area network [IP WAN],

providing of the component of: prior art, a world wide web server [WWW] or web or graphics rich portion of the Internet web server computer,

providing of the component of: prior art, a personal computer [PC], which is non-cryptographically secure,

providing of the component of: prior art, a personal computer [PC] web client,

providing of the component of: prior art, a personal computer [PC] peripherals,

providing of the component of: prior art, a data entry devices of an on-board protected electronic device, toggle field with a prior art liquid crystal display [LCD] for entry of the unique customer passphrase with closely corresponding passcode entry,

providing of the component of: prior art, a data entry device of computer keyboards,

providing of the component of: provided said, new art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-text data sent to an attached provided, said prior art, digital serial bus, furthermore, 1st example means being digitized fingerprint

bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of: prior art, a banked-EEPROM card reader-writer,

providing of the component of: prior art, a personal computer's [PC's] peripheral data storage devices, with means for detachable or removable non-volatile memory units,

providing of the component of: prior art, a personal computer's [PC's] based peripheral data storage media units, with means for archival storage of large amounts of digital data,

providing of the component of: prior art, a cryptographic digital signal processor [C-DSP],

providing of the component of: a new art, a cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through said tamper resistant non-volatile memory,

providing of the component of: new art, cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through provided, said tamper resistant

non-volatile memory [TNV-EEPROM], furthermore, through enhanced cryptographic hardware aids for both secret key and for public key, strong cryptography,

providing of the component of: a new art, programmable gate array logic [GAL] form of high density, application specific integrated circuit [ASIC] with embedded, provided, said cryptographic digital signal processor [C-DSP] structural means, functions as mentioned in the paragraph just above,

providing of the component of: a new art, cryptographic digital signal processor [C-DSP], with structural means for secure cryptographic key storage through said tamper resistant non-volatile memory [TNV-EEPROM],

providing of the component of: prior art, a non-cryptographic micro-processor [uP] or a central processing unit [CPU], with exampled implementation means such as a commercial, 32-bit, Intel Pentium class of micro-processor central processing unit [CPU], with a control unit and on-chip floating point processing unit,

providing of the component of: a new art, a cryptographic computing based unit [C-uP] or a proper superset of provided said, new art cryptographic digital signal processor [C-DSP] structural means, furthermore, having a hardware design implementation of a proper subset or silicon compiler class library selection, of said cryptographic micro-controller [C-u-CTLR], with means for secure handling of strong cryptography keys and auxiliary strong

cryptography hardware aids, furthermore, during system start-up and at customer chosen, periodic intervals, being able to verify physical media loaded and also down-loaded, micro-processor firmware by prior art, cryptography means such as a primitive, smart card loaded, private key digitally signatured, message authentication cipher of the executable program code [EXE CODE] or [PrK[MAC[EXE CODE]]],

providing of the component of: a new art, a cryptographic computing based unit [C-uP], furthermore, having a hardware design implementation of a proper subset or silicon compiler class library selection, of said cryptographic digital signal processing [C-DSP] structural means, with means for secure handling of strong cryptography keys intended for commercial digitally compressed, digital music and movies,

providing of a new art, class of cryptographic computing hardware integrated circuit [C-IC] units or a provided, said cryptographic digital signal processor [C-DSP] structural means, comprising of the above exampled cryptographic digital signal processor [C-DSP] structural means, plus very similar in hardware design given modern grey scales of very cost competitive, digital chip architectures, ranging in relevance, from design bench, custom fuse link programmable, application specific integrated circuits [ASIC'S], all the way in grey scale digital computing complexity, to modern silicon compiler custom designed integrated circuits [IC's] for mass production, as structural implementation hardware means, only illustrated by the above cryptographic hardware units, with functional means for keeping strong cryptography: secret keys,

private keys, family keys, session keys, and often used public keys, secret in secure tamper resistant hardware or red-black hardware, including as a component, said tamper resistant, non-volatile electrically erasable read only memory [TNV-EEPROM], with means of using pass-thru encryption methods over open or wiretapable digital computer system buses to confidentially and securely, transfer said strong cryptography keys into the said hardware from an external wiretapable, input-output serial bus connected source only exampled by a human portable vault functional means, structural means of a smart card, and its own said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], furthermore, also exampled by a remote local area network [LAN] source, furthermore, also exampled by a MODEM connected remote global Internet-Web source,

providing of the component of a new art, cryptographic operating system [C-OS], designed for provided said, cryptographic personal computer (C-PC) having an internal provided said, cryptographic micro-processor unit (C-uP),

providing of the component of: a new art, a non-cryptographic, media player [MP] having internal, provided said prior art, digital signal processors [DSP's],

providing of the component of: a new art, a cryptographic media player [C-MP] structural means, constructed with a provided said, new

art, cryptographic digital signal processor [C-DSP] structural means, having structural means for internal provided said, tamper resistant non-volatile, electrically erasable programmable read only memory [TNV-EEPROM], for playing of customized per customer, strong encrypted digital media,

providing of the component of: a new art, cryptographic media player [C-MP] structural means,, with means for playing back custom secret key encrypted, compressed digital, audio-video in standard format,

providing of the component of: a new art, cryptographic personal computer [C-PC] which is created by using new art, said cryptographic micro-processor [C-uP], with means for digitally processing, new art, custom encrypted digital media,

providing of the component of: a new art, cryptographic personal computer [C-PC] having a subset functionality of said cryptographic micro-processor [C-uP] means, which is created by using a prior art, standard off-the shelf, personal computer [PC] design with a new art, said cryptographic micro-processor unit [C-uP],

providing of the component of: provided said, new art, classes of cryptographic bio-ID input devices [C-BIO-ID-READERS], characterized by using customized, session key, pass-thru encryption for cipher-text data sent to an attached provided, said prior art, digital serial bus, furthermore, attached to a provided, said new art,

cryptographic PC [C-PC], furthermore, 1st example means being digitized fingerprint bio-ID readers, 2nd example means being digitized DNA bio-ID readers, 3rd example means being digitized speech contents, bio-ID readers, 4th example means being digitized hand-writing samples bio-ID readers, 5th example means being facial cognitive features bio-ID readers,

providing of the component of a new art, cryptographic operating system [C-OS], designed for provided said, new art, cryptographic set-top box, having an internal provided said, cryptographic micro-processor unit (C-uP),

providing of the component of: new art, a universal cryptographic set-top box [C-BOX], form of provided said, new art cryptographic media players [C-MP's] for playing back customized digital media,

providing of the component of: a new art, cryptographic micro-mirror module [C-MMM], commercial theater projection-theater sound units which are special cryptographic media players which use prior art, removable permanent memory devices,

providing of the component of: prior art, a modified secure operating system [secure-OS] for world wide web [WWW] server computers which will custom customer session key encrypt a vendor secret key encrypted digital master, and electronically distribute

custom, encrypted digital media masters, using firewalls, using anti-viral software updated weekly, using network protocol converters, using standard layered security methods, and using 'inner sanctum' protection for vendor session key or one-time secret key encrypted digital media masters,

providing of the component of: prior art, a global Internet and world wide web [WWW] based transmission control protocol-internet protocol [TCP-IP] command protocol stack program for Internet connectivity,

providing of the component of: prior art, standard, a plurality of cryptographic mathematics algorithms,

providing of the component of: prior art, a plurality of public key cryptography algorithms which create public keys and private keys,

providing of the component of: prior art, a plurality of secret key cryptography algorithms which create secret keys and session keys or 1-time use only, secret keys, and also play counts or access counts or media decryption counts and play codes or session keys or 1-time use only secret keys,

providing of the component of: prior art, a plurality of hybrid key cryptography algorithms which are combined public key and private key cryptography algorithms,

providing of the component of: prior art, a plurality of private key and secret key splitting algorithms,

providing of the component of: prior art, a plurality of private key and secret key escrow techniques,

providing of the component of: prior art, a plurality of algorithms used to generate: cryptographic keys which are the collective public keys, private keys, secret keys, session keys or 1-time use only secret keys, play counts, play codes, passphrases-passcodes,

providing of the component of: prior art, a plurality of computer cryptography protocols,

providing of the component of: prior art, a plurality of pass-thru encryption algorithms for transmitting secure data over wiretapable computer buses ['red buses'],

providing of the component of: prior art, standardized form, a plurality of lossy compressed digital media algorithms with many prior art example means, and new art emerging future standards,

providing of the component of: prior art, a transmissions control protocol/internet protocol [TCP/IP] for Internet connectivity,

providing of the component of: prior art, a secure internet protocol layer [secure IP layer] layer of Internet data encryption, used in this present patent only as an outer-most security layer which is considered cryptographically un-reliable,

providing of the component of: prior art, a secure sockets layer [SSL] layer of Internet data encryption,

providing of the component of: prior art, a plurality of world wide web [WWW] server standard interchange file language with 1st example protocol being hyper-text mark-up language [HTML], 2nd example protocol being extensible business mark-up language [XBML] also known as [XML], and 3rd example protocol being the most generalized-text mark-up language [GTML],

providing of the component of: a plurality of world wide web [WWW] client standard interchange file languages, with 1st example being hyper-text mark-up language [HTML],

generating of a set of common system keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using provided prior art said public key and secret key cryptography algorithms to generate system cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding of generated said common system keys into each and every provided, said cryptographic digital signal processor [C-DSP] structural means, and also if relevant, a provided said cryptographic integrated circuit [C-IC], furthermore, embedding said common system keys into the said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM] inside of each and every, provided said smart card,

generating of a set of unique per vendor, commonly distributed only in provided, said tamper resistant hardware [TNV-EEPROM], media distribution vendor cryptographic keys eventually used in a provided said, new art, cryptographic digital signal processor [C-DSP] structural means, and also if relevant, a provided said, new art, cryptographic integrated circuit [C-IC] structural means, eventually used in provided, said cryptographic micro-processors [C-uP's] structural means, for eventual manufacturing into provided, said cryptographic micro mirror modules [C-MMM] structural means, involving several processes with a 1st example means being the prior art, provided, said, US National Institute for Standards and Technology's Clipper-Capstone chip with provided, said embedded tamper resistant non-volatile electrically erasable programmable read-only memory [TNV-EEPROM], and a 2nd example means being the provided said, new art, cryptographic digital signal processor (C-DSP) structural means being a prior art, digital signal processor having a silicon compiler designed equivalent of the former's functions [C-DSP] structural means, with added silicon compiler functions for prior art algorithm means for subsequent customer uses of digital signal compression audio-video digital compression means involving several processes and components with 1st example audio-video digital compression means involving several processes being given as prior art, Moving Picture Electronics Group standards X [MPEG X], 2nd example audio-video digital compression means being given as prior art, fast wavelet audio-video compression or convolutional coding compression, 3rd example audio only digital compression example means being given as prior art, MPEG I audio

layer 3 [MP3], and 4th example audio only digital compression example means being given as prior art, fast wavelet audio only compression algorithms [AAC], furthermore, with subsequent customer uses of a prior art, pass-thru encryption means involving several processes and components which are used to transfer said unique customer cryptographic keys over wiretapable or open computer buses ['red buses'] with a 1st example pass-thru encryption means given as common, family key, secret key encryption, a 2nd example pass-thru encryption means given as common family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor public keys followed by the relevant vendor public key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor public keys followed by relevant vendor private key decryption of the received data block, and a 3rd example pass-thru encryption means being a family key encryption of an index to the unique active vendor which references a pre-embedded, common look-up table of unique vendor secret keys followed by the relevant vendor secret key encrypted data which is received on the other end of the computer bus by family key decryption of the vendor index to the same pre-embedded, common look-up table of unique vendor secret keys followed by relevant vendor secret key decryption, for eventual manufacturing into a cryptographic media player, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using prior art algorithms for both public key and secret key cryptography to generate a unique

set of vendor cryptographic keys, while having absolutely no access to any vendor identifications, furthermore, the sub-process of embedding in entirety, said unique set of vendor cryptographic keys in an organizational table form means involving several processes with first example organizational table form means being a unique vendor system key table which is indexed by a vendor identification number, furthermore, said organizational table form means is semi-conductor foundry factory embedded into each and every cryptographic digital signal processor [C-DSP] structural means, while specific vendor private keys and vendor secret keys including a minimum count of one vendor key of the private key of vendor party vn, are factory time embedded into each and every one of vendor party vn's eventually distributed provided, said media ticket smart cards and their internal, provided, said cryptographic micro-controller [C-u-Ctlr] for use in a pass-thru encryption means of several example pass-thru encryption means as explained in a separate process,

generating of a unique media ticket smart card cryptographic key set or also known as a given, unique customer party a's, chosen out of the unique customer parties: a, b, c, i to z's, cryptography key set, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, using provided, prior art algorithms for both public key and secret key cryptography to generate unique customer cryptographic keys, while having absolutely no access to customer identifications, furthermore, the sub-process of embedding into a provided, single said unique media ticket smart card with an embedded cryptographic

micro-processor (c-uP), a unique customer party a's, unique cryptographic key into party a's, eventually distributed provided, said media ticket smart card with its internal cryptographically secure storage of provided, said embedded cryptographic micro-processor [C-uP],

distributing of provided, said cryptographic digital signal processor [C-DSP] structural means, plus provided, said cryptographic micro-processors [C-uP] contained in provided said, cryptographic micro-mirror modules [C-MMM's], furthermore, the distributing of said cryptographic digital signal processor [C-DSP's] structural means, is based upon the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing provided, said cryptographic digital signal processor [C-DSP] structural means, to individual media distribution vendors for manufacturing into vendor party vn's cryptographic micro-mirror module [C-MMM] structural means, while having absolutely no access to whole cryptographic keys and having unique vendor party vn access to only his own unique vendor secret key vn, and unique vendor private key vn, with its unique, matching public key vn,

distributing of the factory cryptographically programmed, provided, said media ticket smart cards, which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors for selling to customer parties: a, b, c, i to z, while having absolutely no access to whole cryptographic keys,

escrowing of the split cryptographic keys which is the process done by the central public key generation authority, party g, safe-guarding the split cryptographic customer keys, and split cryptographic vendor keys contained in provided, said prior art relational databases, kept in an entirely secure and confidential manner, for achievement of legal means involving several processes, with a 1st example legal means being simple customer identification and lost cryptographic key recovery, a 2nd example legal means being court ordered only, disputed ownership cryptographic key recovery, and a 3rd example legal means being court ordered only cryptographic key recovery use by law enforcement,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with a minimum of 3-layers of digital computer architecture: a relevant patent drawing's bottom-most layer composed of the media ticket smart card system authority, a central layer composed of authorized media distribution companies labeled as parties vn, and a top-most layer or user layer composed of customer parties a, b, c, i to z,

preparing of a unique play code and a unique play count which is the process done by the authorized digital media distribution unique vendor company, party vn, preparing said unique play code [a session key or one-time use secret key], and said unique play counts [a paid for number of plays or count of free trial plays], and preparing of the custom encrypted digital media for downloading to each customer,

downloading to given, unique customer party a, out of customer parties: a, b, c, or i to z, at a private dwelling, prior art, insecure ['red bus'], personal computer [PC] which is the process done by the authorized digital media distribution vendor, party vn, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a prior art, provided, world wide web [WWW] server over the global Internet to multiple prior art, provided, personal computer [PC] based web clients, one of whom is customer party, a, b, c, or i to z, of encrypted play codes or one-time use only, secret keys or session keys) with header and encrypted play counts or paid for counts of plays or decryptions or counts of free trial plays, with header for deposit into said factory cryptographically programmed, provided, said prior art, media ticket smart cards, attached to a provided, said prior art, personal computer [PC based] media ticket smart card readers, and one-way transfer of custom session key or one-time use only secret-key encrypted pre-unique vendor secret key encrypted digital media for deposit into physical digital media inserted into media drives attached to provided, said prior art, personal computers [PC's] owned by customers,

delivering by foot which is the process done by the given, unique customer party a, of physically transferring both physical custom encrypted digital media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, provided, said prior art, personal computer [PC], to any other customer party's: a,

b, c, or i to z, provided, said cryptographic media player [C-MP] structural means,, with its embedded said cryptographic digital signal processor [C-DSP] structural means, also with a built-in media ticket smart card reader,

encrypting in a pass-thru manner for media ticket smart card upload to a provided said, new art, cryptographic micro-mirror module [MMM] with its provided, said cryptographic digital signal processor [C-DSP] structural means, using pass-thru encrypting means involving several processes and components for transferring any type of digital data securely from originating said media ticket smart card up to answering provided, said cryptographic digital signal processor [C-DSP] structural means, with a 1st example pass-thru encrypting means being said common family key or shared secret key encryption which is known to be vulnerable to a single point of attack, a 2nd example pass-thru encrypting means being originate vendor, unique, vendor private key digital signaturing to 'signatured-text,' not being encrypted text, thus readable by any party who easily obtains the public key, followed by answering vendor, unique, vendor public key digital public key encryption to 'cipher-text' or encrypted text, using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being a row, column table indexed by a vendor identification number, a 3rd example structural means of pass-thru encrypting means, being originate vendor, unique, vendor secret key encryption to 'cipher-text (encrypted text which combines signaturing)' using said pre-

embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being a row, column table indexed by a vendor identification number,

encrypting in a pass-thru return manner for said cryptographic media player's prior art, provided, said cryptographic micro-mirror machine module [C-MMM] structural means, with its provided, said internal, cryptographic digital signal processor [C-DSP] structural means, download to said media ticket smart card using pass-thru encrypting return means involving several processes and components for transferring any type of digital data securely from said cryptographic digital signal processor [C-DSP] structural means to said media ticket smart card with a 1st example pass-thru encrypting return means being common family key or shared secret key encryption which is known vulnerable to a single point of failure, 2nd example pass-thru encrypting return means being answer vendor unique private key digital signaturing to 'signatured-text' or digitally signatured text which is non-encrypted, and thus readable by any party, followed by originate vendor unique public key encryption to 'cipher-text' or encrypted text using said pre-embedded, common look-up table of unique vendor public key and matching private keys with organizational means involving several processes and components such as first organizational means being the row, column table indexed by a vendor identification number, a 3rd example pass-thru encrypting return means being answer vendor unique secret key encryption to 'cipher-text' or encrypted text, which combines digital signaturing

by using said pre-embedded common look-up table of unique vendor secret keys with organizational means involving several processes and components with first organizational means being the row, column table indexed by a vendor identification number,

initializing before playing which is the process done by the given customer, party a, of preparing any customer party's: a , b, c, g, i to z's, personally owned provided, said cryptographic micro-mirror machine module [C-MMM] structural means, with its internal provided, said cryptographic digital signal processor [C-DSP] structural means, by inserting his own party a's unique custom encrypted digital media, and also by inserting his own party a's unique provided, said media ticket smart card,

transferring of the cryptographic keys from the prior art, provided, said media ticket smart card to provided said, new art, cryptographic micro-mirror module [C-MMM] structural means with its provided, said cryptographic digital signal processor [C-DSP] structural means, by use of said pass-thru encrypting means, of the unique customer cryptographic keys over wiretapable or open computer buses ['red buses'] which is the process done by the cryptographic media player to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n which are pass-thru encrypted by the several pass-thru encryption means involving several processes and components for transfer over wiretapable computer buses ['red buses'] to the player's own cryptographic memory [TNV-EEPROM] for access by its provided, said cryptographic digital signal processor [C-DSP] structural means, with

said 1st example pass-thru encryption means being the common family key encryption vulnerable to a single point of attack, a said 2nd example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said 3rd means of pass-thru encryption being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access,

transferring of the cryptographic keys away from provided said, new art, cryptographic micro-mirror module [C-MMM] structural means, with its internal provided, said cryptographic digital signal processor [C-DSP] structural means, to provided, said prior art, media ticket smart card, by use of pass-thru encrypting return means, of the unique customer cryptographic keys over wiretapable or open computer buses ['red buses'] which is the process done by the cryptographic media player which are pass-thru encrypted by the several pass-thru encryption means for transmit using it's provided, said new art, cryptographic digital signal processor [C-DSP] structural means, the encrypted play codes with header and encrypted play counts with header both with provided, said new art, cryptographic digital signal processor [C-DSP] structural means of incremented sequence counts (to avoid recorded replay attacks without the use of synchronized digital clocks) to the media ticket smart card a, transferred over wiretapable computer buses, with said 1st example pass-thru encryption

means being the common family key encryption vulnerable to a single point of attack, a said 2nd example pass-thru encryption means being the pre-embedded, common, look-up table of vendor private keys and matched public keys which uses a family key encrypted, common table index for efficient active table entry access, a said 3rd example means of pass-thru encryption being the unique vendor secret key encryption with use of a common, look-up table of vendor secret keys which uses a family key encrypted, common table index or vendor ID number for efficient active table entry access,

authenticating using media triangle authentication which is the process of matching the unique digital media with its matching unique play code by the method done by said cryptographic micro-mirror modules [C-MMM] structural means internal, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, doing digital media triangle authentication using sample reads of test data with successful decryption,

cryptographing using hybrid key cryptography which is the process done by provided said, new art, cryptographic micro-mirror modules [C-MMM's], internal provided, said new art, cryptographic digital signal processor [C-DSP] structural means, using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys [ssk-n], used for only one session, which said session keys are sent to a remote party who decrypts them for storage

in his own provided, said tamper resistant, non-volatile memory [TNV-EEPROM] embedded on his provided, said cryptographic digital signal processing [C-DSP] structural means, with a 1st example means of the provided said, new art, cryptographic digital signal processor [C-DSP] structural means, and a 2nd example means of a provided, said cryptographic integrated circuit [C-IC], which said 1-time use only secret keys or session keys, may be later stored in provided, said tamper resistant non-volatile memory [TNV-EEPROM], embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts,

accounting by provided said cryptographic micro-mirror module [C-MMM] structural means, with its internal, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, which is the process done using hybrid key cryptography digital media playing of one-way transfer of custom session key encrypted digital media, owned by unique customer party a, in a controlled access manner mostly for financial accounting purposes which uses the play codes [session key or one-time secret key] and play counts [paid for number of plays or count of free trial plays] contained in media ticket smart cards,

playing by provided, said cryptographic micro-mirror module [C-MMM] structural means with its internal provided, said new art, cryptographic digital signal processor [C-DSP] structural means, which is the process done using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes or session key or one-

time use only, secret keys, and play counts or controlled re-play counts, now contained within registers in the provided, said cryptographic digital signal processor [C-DSP] structural means, and also the hardware secret key double decryption directly used upon the custom encrypted, one-way transfer of custom session key encrypted digital media, which is pre-unique vendor secret key encrypted, using first the unique customer session key decryption and then the unique vendor secret key decryption with sequence number checks for countering recorded replay attacks,

escrowing retrieval of lost, stolen, or disputed legal ownership media ticket smart cards, as well as custom cipher text, digital media distribution material, which is the process done by the unique customer, party a, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of 'de facto' standards, leading up to internationally standardized cryptography sanctioned by industry trade groups such as the Recording Industry Association of America's [RIAA's] Secure Digital Music Initiative [SDMI], the National Association of Broadcaster's [NAB's] Secure Digital Broadcast Group [SDBG],

whereby the present invention has implemented in process claims, through the minimal said 3-layer federated system of cryptographic layers for wider claims coverage by condensing the 2 of 4, middle-most layers of the relevant patent drawing's 4 cryptography layers, into a

combined for claims purposes: low-middle layer for commercial hardware vendors, plus a high-middle layer for commercial digital media vendors, a process is by this claim implemented of a design rule of having: no inherent hardware and firmware secrecy, no hidden wiretapping points, and also no double key spaces, furthermore, the minimal said 3-layer federated system of cryptographic layers of this invention's layers: the bottom-most relevant patent drawing's cryptographic system architecture layer of said system keys under said system party s, in which this system party s's administration through said whole key generation party g, who has been given 100% whole key knowledge, but, 0% knowledge of customer identifications, furthermore, party s also having said whole key distribution party d, who has been given 0% whole key knowledge, but, 100% knowledge of customer identifications [ID's], who has been administer of provided, said cryptographic integrated circuit classes [C-IC] hardware distribution process, which has enabled only limited, trusted national commercial, cryptographic hardware vendors [C-IC's], who are legally allowed by party d, to firmware program with confidential system cryptographic keys, said tamper resistant non-volatile memory (TNV-EEPROM) of each said cryptographic integrated circuit classes [C-IC], in order to keep said system keys top secret, furthermore, at the relevant patent drawing's, low-middle level said relevant patent drawing's layers, of system hardware world-wide distribution under administration of said party d, said PC cryptographic hardware plug-in board classes of hardware vendors, are simply given by said system authority distribution party d, 100% pre-programmed with cryptographic system keys, said, tamper resistant non-volatile memory [TNV-EEPROM] which is pre-stored inside of centrally

distributed, said cryptographic integrated circuit device classes [C-IC's], used to install in their PC peripheral device hardware, furthermore, at the relevant this process claim's, high-middle cryptographic layer of said party d administered, digital media distribution vendor parties vn, the cryptographic layer of commercial system administrators having vested commercial interests with their own commercial industry groups, furthermore, desirably aided in commercial secrets enforcement by future, commercial anti-espionage felony laws, furthermore, at the relevant this process claim's, top-most cryptographic layers of said, customer parties: a, b, c, i to z, and given customer a, and his unique per customer a, only said smart card a, distributed and securely protected by said tamper resistant non-volatile electrically erasable programmable read only memory [TNV-EEPROM], cryptographic keys, are known only to the relevant this claim's, high-middle layer digital media distribution vendor parties vn, contained within secure, optional by dependent claim, key industry layers of commercial, split key escrow databases, alltogether implementing a highly federated cryptography system,

whereby the present invention has created several processes for doing unique, customer custom session key or one-time secret key encrypted copies of initially unique, vendor secret key encrypted, digital media distribution over the prior art, insecure ['red bus'] Internet using secure, World Wide Web [WWW] ['black'] servers involving the cryptographically secure transfer ['download'] from Web server to customer prior art, personal computers [PC's] over insecure ['red bus'] Internet connection lines, of custom encrypted, digital media to prior

art, standard form recordable media, and also custom decryption cryptographic keys or play codes, and custom pre-programmed accounting counts or play counts, for deposit onto provided, said prior art, smart cards, called media ticket smart cards,

whereby the present invention has created several processes for securely physically transferring ['footprint download'] of both said custom, encrypted digital media on standard form recordable media along with the customer's universal media ticket smart card for all vendors and all digital media to said cryptographic micro-mirror modules [C-MMM's], with internal provided, said prior art, said cryptographic digital signal processors (C-DSP's), for media playing which are universally and uniquely, pre-programmed for every authorized vendor participating in the system, and can also accept any authorized, unique customer's smart card which must have relevant play codes and play counts for upload and use which are both uniquely matched to the authorized custom encrypted digital media inserted for playing,

whereby a highly federated or regional cryptography architecture has been commercially implemented by commercial industry organizations, proximately in human corporate organization, corresponding to today's US based, prior art, magnetic strip credit card management and distribution industry group associations, with corresponding EU based prior art, smart card commercial corporate organizations, furthermore, implementing through the process of this patent, over the global Internet-Web, individual human level and corporate body human level, trust granting policies known as a relative, two-way, middle level individual-organizational trust granting model, or a middle level trust

model, versus, earlier highly centralized, 100% top-down trust granting models exampled by the US Federal National Institute of Standard's (NIST's) Clipper chip and Capstone program, versus, earlier 100% bottom-up trust granting models, often called tangled web of trust models,

whereby Moore's Law of industrial engineering in semi-conductor device fabrication has been reasonable compensated, especially regarding future expansions in capacity of provided, said tamper resistant non-volatile, electrically erasable programmable read-only memory [TNV-EEPROM],

whereby the present invention has allowed using several of the above systems processes in safeguarding relative, commercial value, of multi-million dollar digital masters released by vendors through global World Wide Web (WWW) distribution.

103. The process of claim 102 whereby the process of authenticating by customer triangle authentication which is the process done by the 3 geometric points of: point 1: provided said, new art, smart card with bio-ID, point 2: given customer party a of customer parties: a, b, c, i to z, and point 3: an authorized provided, said new art, cryptographic micro-mirror module [C-MMM] structural means, with its internal, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, furthermore, which process step may be skipped for low security only when customer time and effort is of the essence,

whereby this process claim has achieved, relatively hacker resistant, strong verification of parties involved, comprising the minimal of, 3 referenced geometric points comprising of a minimal 3-sided, geometric triangle with strongly, associated parties n, pn, are uniquely identified and the given customer party a, out of customer parties: a, b, c, i to z, are customer party a warned for any mis-matches of customer smart card a with a 1 to N mapping of smart card a, to N possible counts of custom cipher text digital media, physically inserted or physically playable in provided, said cryptographic micro-mirror module [C-MMM] structural means, in a high probabilistic manner, while accomplishing anti-fraud security actions.

104. (NEW) The process of claim 102 whereby the process of public key cryptographing is done for authentication by provided, said new art, cryptographic micro-mirror module [C-MMM] structural means, with its internal, provided, said new art, cryptographic digital signal processor [C-DSP] structural means, using prior art, public key cryptography algorithms which is the process of using public key cryptography authentication, encryption, and decryption using public keys [puk-n], and private keys [prk-n], stored within provided, said tamper resistant non-volatile memory [TNV-EEPROM] embedded within non-wirelapable ["black"] cryptographic computing units in the example of provided, said new art, cryptographic digital signal processors [C-DSP] structural means,

whereby the involved parties have achieved by this process claim, very low probability of hacker intercept, remote strong authentication of involved parties, plus remote relatively slow execution speed public key encryption and decryption, by use of provided, said prior art, public key cryptography algorithms, executed inside of provided, said new art, cryptographic micro-mirror modules [C-MMM] structural means.

105. (NEW) The process of claim 102 whereby the process of secret key cryptographing uses prior art, secret key cryptography which is the process done by provided, said new art, cryptographic micro-mirror module [C-MMM] structural means having internal, provided, said cryptographic digital signal processor [C-DSP] structural means, using secret key cryptography which is the process of using secret key cryptography with a non-wiretapable ["black"] bus, cryptographic computing unit in structural means, exampled by a provided, said new art, cryptographic digital signal processing [C-DSP] structural means, furthermore, using 1-time use only secret keys [sek-n] or session keys [ssk-n], stored upon provided, said tamper resistant, non-volatile memory [TNV-EEPROM], using the following sub-process:

cryptographing using fast hardware session key cryptography which is the process done by a provided, said new art, cryptographic digital signal processor [C-DSP] structural means, internal to a provided, said new art, cryptographic set-top box [C-BOX], using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ["black"], provided, said new art, cryptographic digital signal processing [C-DSP] structural means, with access to higher security level, provided, said tamper resistant non-volatile [TNV-EEPROM] ["black"]) memory for cryptographic key storage of private keys and secret keys, which

hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key cryptography encryption and decryption of block transferred digital media,

whereby this process claim has achieved for the involved parties, a very low probability of hacker intercept, very fast and high efficiency, provided, said prior art, secret key cryptography algorithm communications inside of a provided, said new art, cryptographic micro-mirror module [C-MMM] structural means.